



ビットコイン・ディプロマ

ビットコイン時代の金融教育

生徒用ワークブック

日本語版 | 2025年版

My First Bitcoin has created this work and made it
freely available under **Creative Commons**.

This work is licensed under
Creative Commons
Attribution-ShareAlike
4.0 International (CC BY-SA 4.0)



ビットコイン・ディプロマ

ビットコイン時代の金融教育

生徒用ワークブック
日本語版 | 2025年版



DONATE NOW

bctq5ey66ppn7gj6p0432x0re0j43kdr7jzrd54gnw3yrc3dw8dqcw9pwsd

ビットコイン・ディプロマ（Bitcoin Diploma）の軌跡

機が熟したアイデアほど、強力なものはありません。

ビットコイン・ディプロマの物語はエルサルバドルで始まりました。

2022年6月、公立学校の生徒38名が最初のパイロットプログラムを修了。

これは、世界で初めて公立学校制度の中で実施されたビットコイン・ディプロマ（卒業証書）でした。

それがわずか3年前のことだとは信じがたいことです。

その後の成長は目覚ましく、全国で何千人の卒業生を輩出しています。

さらに嬉しいのは、この取り組みが私たち以外の人々の手によっても広がっていることです。

ワークブックはオープンソースであり、エルサルバドル国内外の多様なビットコイン教育者がこれを活用しています。

エルサルバドル教育省は、このワークブックを独自のビットコイン・ディプロマの主要教材として採用。

2024年にはBitcoin Beachと提携し、400人を超える公立校の教師に研修を提供し、

各学校での授業実施を後押ししました。

当初の目標の一つは、国家規模で教育を行い、ビットコイン教育が社会にとって大きな善の力となることを示すことでした。

その夢は、いま確実に形になりつつあります。

エルサルバドルが中心でありながら、私たちの使命は世界に広がっています。

2023年3月には、国際的な「Bitcoin Educators Node Network」を設立。

参加ノードは以下の原則に同意することを求めています。

“教育が、独立性、公平性、コミュニティ主導、ビットコインのみ、高品質、そしてエンパワーメントを重視していること”

この自律ネットワークでは、現在までに8言語以上に翻訳され、以下の国々でビットコイン・ディプロマが実施されています。

抜粋：

カナダ、米国、メキシコ、グアテマラ、ホンジュラス、コスタリカ、キューバ、ドミニカ共和国、ハイチ、コロンビア、スリナム、ペルー、ブラジル、アルゼンチン、アイルランド、英国、ポルトガル、ジョージア、ガーナ、ナイジェリア、ウガンダ、ケニア、ザンビア、ジンバブエ、南アフリカ、アフガニスタン、バングラデシュ、インド、香港、インドネシア、オーストラリアなど。

ネットワークは毎月新しいノードが追加されており、オープンソースであるため、誰にも許可は必要ありません。完全に独自で実施している組織も多数あるでしょう。

これは、世界規模の分散型ムーブメントです。

独立した、中立的な、コミュニティ主導のビットコイン教育は世界を変えます。

すでにその変化は始まっているのです。

より良い世界のために

My First Bitcoin team -
2025

目次

第1章：なぜ私たちは「お金」が必要なのか？

1.0 はじめに	01
1.1 サトシと学ぼう	01
アクティビティ：お金に関する5つの質問	01
1.2 クラスディスカッション－なぜ私たちはお金が必要なのか？	04

第2章：お金とは何か？

2.0 はじめに	07
アクティビティ：クラスディスカッション－お金とは何か？	07
2.1 お金の定義	07
2.2 お金の機能	09
2.3 お金の性質	10
2.4 お金の種類	13
2.5 お金の心理学：希少性、時間選好、トレードオフ	14
アクティビティ：時間選好	16

第3章：お金の歴史

3.0 はじめに	21
アクティビティ：物々交換ゲーム	21
3.1 物々交換から現代通貨への進化	23
3.1.1 初期のお金の抱えていた問題	23
3.1.2 硬貨と紙幣の発展	24
3.1.3 健全な通貨から不健全な通貨への移行	25
3.1.4 紙からプラスチックへ	27
3.2 デジタル通貨	28

第4章：法定通貨とは何か？誰が管理している？

4.0 はじめに	31
4.1 法定通貨の簡単な歴史	31
4.2 法定通貨システム	34
4.2.1 法令によって成り立つ金融システム	34

4.2.2 部分準備銀行制度：負債によって支えられる仕組み	35
アクティビティ：部分準備銀行制度	38
4.2.3 誰が法定通貨システムを管理していて、どのような利益を得ているのか？	39
4.3 中央銀行デジタル通貨（CBDC）：法定通貨の未来	41

第5章：問題は解決策を生む

5.0 問題の紹介	45
5.1 購買力の低下	45
5.1.1 通貨インフレと購買力への影響	45
アクティビティ：インフレの影響—オークション活動	46
5.2 世界的な債務負担と社会的不平等	47
5.2.1 個人への影響—購買力の喪失	47
5.2.2 社会への影響—富の格差の拡大	52
アクティビティ：法定通貨システムの結末	53
5.2.3 世界的な債務負担	54
5.3 サイファーパンクと分散型通貨の探求	55
5.3.1 サイファーパンク	56
5.3.2 中央集権型システムと分散型システム	57
5.3.3 デジタル通貨の簡単な歴史	59

第6章：ビットコイン入門

6.0 サトシ・ナカモトとビットコインの誕生	63
6.1 ビットコインはどのように機能するのか？	65
6.1.1 ナカモト・コンセンサス・メカニズム	65
6.1.2 ゲームプレイヤーたち	67
アクティビティ：ピア・ツー・ピア（P2P）ネットワークにおける合意形成	69
6.2 健全なデジタルマネーとしてのビットコイン	71
6.2.1 はじめに	71
6.2.2 ビットコインの特徴	72
アクティビティ：クラスディスカッション—ビットコインは「健全なお金」か？	76
6.2.3 自己責任を受け入れる	76

第7章：ビットコインの使い方

7.0 はじめに	81
7.1 ビットコインの入手と交換	81
7.1.1 P2P：対面での取引	81
7.1.2 P2P：オンラインでの取引	82
7.1.3 中央集権型取引所	82
7.2 ビットコインウォレット入門	83
7.2.1 セルフカストディ型ウォレットvsカストディ型ウォレット	83
7.2.2 ビットコインウォレットの種類	85
7.2.3 オープンソースvsクローズドソース	86
アクティビティ：bitcoin.orgでのビットコインウォレットの評価	87
7.3 モバイルビットコインウォレットの設定	87
アクティビティ：ウォレットの設定／復元	87
7.4 受け取りと送金の方法	89
アクティビティ：ビットコイン送受信の実践	91
7.5 ビットコインで貯蓄する	93
7.6 Don't Trust, Verify - 信じるな、検証せよ	94

第8章：ライトニングネットワーク：日常生活でビットコインを使う

8.0 はじめに	97
アクティビティ：「ビットコイン ライトニングネットワーク解説動画：実際の仕組み」を視聴	98
8.1 ライトニングネットワーク	98
8.2 ライトニングウォレットの種類	100
8.2.1 セルフカストディウォレットvsカストディ型ウォレット	100
8.2.2 オープンソースvsクローズドソース	100
8.3 ビットコイン・ライトニングウォレットの設定	100
8.4 ライトニングでの送受信	102
アクティビティ：ライトニングウォレット・リレーレース	106
8.5 ビットコインでコーヒーや食料品を買う	107
8.5.1 オンライン：ECサイトでの決済プラグイン	108
8.5.2 対面：地域の対応店舗を探す	109
8.5.3 一時的なツール：ギフトカード・決済に使えるカード	110
8.5.4 循環型経済と交換手段としてのビットコイン	110

第9章：ビットコインの技術的な仕組み入門

9.0 はじめに	115
アクティビティ：「ビットコインの内部構造の仕組み」動画を視聴	115
9.1 公開鍵と秘密鍵：暗号技術によるセキュリティ	116
9.1.1 公開鍵／秘密鍵を用いた暗号技術	116
9.1.2 ハッシュの仕組み	119
アクティビティ：SHA-256ハッシュの生成	121
9.2 UTXOモデル	122
9.3 ビットコインのノードとマイナーの詳細	125
9.3.1 ビットコインノードとは？ノードの構築方法	125
アクティビティ：ビットコインノードに関する動画を視聴	126
9.3.2 ビットコインマイナーとは？マイニングはどのように機能するのか	126
9.4 mempoolとは？	132
アクティビティ：mempool	134
9.5 ビットコイン取引の開始から終了までの仕組み	135

第10章：なぜビットコインなのか？

10.0 はじめに	139
アクティビティ：ビットコインの未来はどのようなものになるだろうか？	139
10.1 中央銀行デジタル通貨（CBDC）とは？誰が管理しているのか	140
10.2 ビットコインの哲学	141
アクティビティ：クラスディスカッション—あなたには自分のお金を管理する権利があるのか？	141
10.3 ビットコインの利点	142
10.4 力を得た未来	143
アクティビティ：クラスディスカッション—あなたの視点はどう変わった？	143
追加資料	147
各章のコンセプト	149
用語集	153

ビットコイン・ディプロマ

独立した、
公平で質の高い、
そして無料の教育による
10週間の変革の旅

ビットコインを学ぶ前に、「お金」の基本、その歴史、
そして現在の金融システムをしっかりと理解しておくことが不可欠です。
これらの概念を押さえることで、
ビットコインの独自性や破壊的な性質をとらえるための確かな土台が築かれます。

お金の進化の過程を知れば、現在の金融システムが持つ可能性と限界、
そしてビットコインがどのようにそれらに挑もうとしているのかが、
より明確に見えてくるでしょう。

このような基礎知識がなければ、ビットコインの本質や、
その社会にもたらし得る影響を十分に掘り下げることは難しいかもしれません。

あわてず、じっくりと学びを進めていってください。
この最先端の分野をより深く探求し、その核心に触れるることは、
きっとかけがえのない体験になるはずです。

第1章： なぜ私たちは 「お金」が必要なのか？

1.0 はじめに

1.1 サトシと学ぼう

アクティビティ：お金に関する5つの質問

1.2 クラスディスカッション－なぜ私たちはお金が必要なのか？

生徒用ワークブック

日本語版 | 2025年版

なぜ私たちは「お金」が必要なのか？

1.0 はじめに

お金とは、人類が発明した中で最も偉大な自由の手段のひとつである。

フリードリヒ・ハイエク

ようこそ、ビットコイン・ディプロマへ。
この章では、「なぜお金が私たちの生活に不可欠なのか？」という根本的な問い合わせていきます。
お金の本質やさまざまな形について学び、その重要性をより深く理解することを目指します。

お金は、私たちがほぼ毎日使っているものですが、「なぜ必要なのか」「それが何なのか」を本当に理解しているでしょうか？

なぜ私たちの両親や家族は、自分の時間をお金と交換しているのでしょうか？

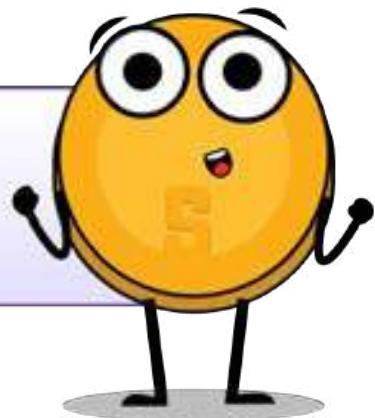
なぜある人はたくさんのお金を持ち、他の人はそうでないのでしょうか？

なぜ国によってお金の形が違うのでしょうか？

なぜ必要なときに、お金をもっと作ることができないのでしょうか？

1.1 サトシと学ぼう

こんにちは！サトシだよ。
このビットコイン・ディプロマを通じて、案内役として
あなたをサポートするアシスタントなんだ。
重要な概念を深く理解できるように、
資料や役立つ情報を届けするよ！



アクティビティ：お金に関する5つの質問

食べ物などの生活必需品や、欲しいものを手に入れるなど、お金の実際の使い方を考えてみましょう。
現実的にありそうなことと、少しユニークな自分なりのアイデアをバランスよく取り入れて、
具体的に書いてみてください。

第1章

なぜ私たちはお金が必要なのか？

お金とは何か？

なぜ私たちは「お金」が必要なのか？

誰がお金を管理しているのか？

お金に「価値」を与えているものは何か？

第1章

お金について、あなたが持っている疑問は何ですか？
クラスで共有するために、あなたの質問を書き出してください。

クラス全体で議論を広げ、リストを共有・比較しながら、
お金が必要な理由の中でも特に重要な5つを選び出しましょう。
クラス全体で共通する考えを見つけてください。
また、あなたの意見が選ばれなかったとしても、あなたならではのユニークなアイデアを振り返り、
気づいたことをメモしておきましょう。

1.2 クラスディスカッション – なぜ私たちはお金が必要なのか？

グループで以下の活動をしましょう：

- ◆ 最初の4つの質問について考え方を共有し、話し合いながら、気に入った考え方をメモしましょう。
- ◆ 最後の質問についての考え方を共有し、クラスで最も良いと思う質問を投票で選びましょう。
- ◆ その結果をメモしてください。
- ◆ ビットコイン・ディプロマの最後に、これらの考え方や質問を振り返りましょう。

お金がなぜ必要なのかを考えてみたところで、これからこの章では「お金とは何か」「どのように進化してきたのか」「誰がお金に影響を与えているのか」、そして「お金の最新の形」について学んでいきます。今日作成したリストを時々見返しながら、自分の気づきとお金の生成・定義・使われ方の変化を結びつけて考えてみましょう。

第2章： お金とは何か？

2.0 はじめに

アクティビティ：クラスディスカッション — お金とは何か？

2.1 お金の定義

2.2 お金の機能

2.3 お金の性質

2.4 お金の種類

2.5 お金の心理学：希少性、時間選好、トレードオフ

アクティビティ：時間選好

生徒用ワークブック

日本語版 | 2025年版

お金とは何か？

2.0 はじめに

お金とは、将来ほしいものを手に入れられるという保証である。
今は何も必要としていなくても、新たな欲求が生まれた時にそれを満たす可能性を確保してくれる。

アリストテレス

前章では「お金がなぜ必要なのか」を考えましたが、この章では「お金とは何か？」という根本的な問いに踏み込みます。まずはグループディスカッションとアクティビティから始めましょう。

アクティビティ：クラスディスカッション お金とは何か？

- ◆ ちょっと想像してみて！目の前の机の上に、あなたのキャンディが置かれているとしよう。……まだ食べちゃダメだよ！
- ◆ このキャンディ、100円と交換してもいいよっていう人、いるかな？
- ◆ じゃあ、ボードゲームのモノポリーのチップと交換だったら、どう？
- ◆ なぜそう思うんだろう？
- ◆ どうして一方のお金には価値があるとされて、もう一方は価値がないとみなされるんだろう？
- ◆ 何が「お金」に価値を与えてるのかな？
- ◆ お金って、どこから来て、誰がどれくらい印刷するかを決めているんだろう？
- ◆ もっとお金を印刷して、みんなに同じだけ配ればいいと思わない？
……なぜ、それをしないんだろう？

この2つのお金の決定的な違いは、「一方がもう一方よりも価値がある」と、あなたが信じているかどうかなんだよ。



2.1 お金の定義

お金とは何か、立ち止まって考えたことはありますか？お金がなぜお金なのか、不思議に思ったことはありませんか？お金の使い方は知っていても、お金の出所や仕組みを理解している人はそう多くありません。

お金は基本的に、モノやサービスを交換するための手段です。さまざまな形の品目の価値を、簡単にやりとりできる形で表しています。

お金は紙幣や金属のコイン、電子決済など、さまざまな形があります。

通常、政府やその他の機関がお金を発行・管理していますが、お金は単なる物理的またはデジタルな交換媒体にとどまりません。言語や文化が異なるとしても、世界中の人々との取引に利用できる「共通言語」のようなものもあります。

例えば、世界の反対側にいても、商品をカウンターに置いて現地の通貨と交換したり、クレジットカードで支払ったりすれば、「お金」という共通手段で意思疎通ができるのです。

第2章

お金とは、物々交換に頼ったり、「自分の持っているものをちょうど欲しがっている人」を探したりする必要なしで、取引を可能してくれる“社会的な約束”的なものです。

たとえば、ある集団がチョコレートを商品やサービスの支払いに使いはじめたら、チョコレートはお金として機能するようになります（ただし、溶けてしまう地域もあるので、「悪貨（bad money）」とみなされるかもしれません）。

フランスの経済学者ジャン＝バティスト・セイはこう言いました。

“お金は交換の中で一時的な役割を果たすだけで、取引が完了したときには、ある商品が別の商品と交換されたに過ぎないのです。”

つまり、お金そのものは人間の欲求を満たしてくれるわけではなく、あくまで物々交換を成立させるための“道具”なのです。



取引（トランザクション）とは、商品やサービスの交換や移転のことです。

これは、2者以上の間で「価値を交換する」手段でもあります。

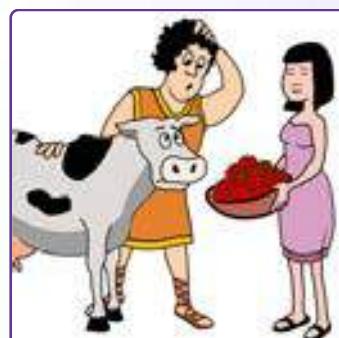
取引にはさまざまな種類があり、例えば「サンドイッチを買う」といったシンプルなものから「家を買う」「株や債券に投資する」といった複雑な金融取引もあります。

対面・電話・オンラインや、それ以外の方法で取引が可能です。関わる相手も、個人・企業・金融機関など多岐にわたります。

お金がなかったら、この取引ってどれくらい簡単に実現できると思う？

例えば、牛1頭とイチゴ100万個を交換する？

それとも60万個？5万個だったらどうかな？



このショート動画もチェックしてね！



お金とは、モノを交換するための基準となる価値であって、モノと交換するために欲しいと思う「価値そのもの」ではありません。

お金の役割まとめ：

- ・みんなが最終的な支払い手段として受け入れているため、取引をスムーズにしてくれる
- ・モノやサービスの価値を測ったり、比較したりすることができる

次は、お金の機能について見ていきましょう。

お金とは何か？

2.2 お金の機能

商品やサービスの売買に欠かせないのが「お金」です。
お金は、世界中でいくつかの重要な機能を果たしています。

1 価値の保存 (Store of Value)

お金は時間が経ってもその価値を保つべきものであり、人間の労働の価値を貯蓄し、投資する手段として役立ちます。これにより、人々はお金を使って将来の計画を立てたり、お金を貸し借りしたりできます。もし何か特別なもののためにお金を貯めている時は、「お金は単なる支払い手段ではなく、将来に向けた計画や投資を助けるツール」だととらえるようにしましょう。

あなたにとっての 「価値の保存」 は何ですか？	BTC (米ドル)	金 (米ドル)	米ドル (ユーロ換算)
2019年3月14日	\$3,846	\$1,293	€0.8817
2020年3月14日	\$5,258	\$1,529	€0.90056
損益	+36.71%	+18.25%	+2.14%

2 交換の手段 (Medium of Exchange)

お金があれば、「自分の持っているものを欲しがる相手」を探す必要がありません。
お金を使えば欲しいものを自由に売買できます。
これにより、取引や商業ははるかに便利で効率的になります。



3 価値の尺度 (Unit of Account)

お金は、さまざまな商品やサービスの価格を表現・比較するための共通の基準を提供してくれます。
これにより、人々は何を売買するかについて情報に基づいた判断ができ、より効率的で透明性のある市場が成り立ちます。

価値の尺度

「価値の尺度」っていうのは、何かに値段（お金の価値）をつけたときに、消費者がそのモノの価値を認識できるってことなんだ。

The illustration features a large, yellow, anthropomorphic coin character with a smiling face, arms, and legs. It is holding a smartphone in its right hand, which displays a soccer ball. To the right of the phone, there are two speech bubbles containing the numbers "2,900円" and "35,000円". In the background, there is a soccer ball and a football.

第2章

考えてみよう：

もし新車を買いたいと思ったら、さまざまな販売店で価格を比較し、情報に基づいてどの車を買うか判断できます。でも「価値の尺度」がなければ、別の基準で比べるしかありません。例えば、「その車が何頭分の牛に相当するか」や、「車を作るのにどれだけの時間がかかったか」で比較することになります。

価値の保存・交換の手段・価値の尺度。

これら3つの機能が、経済を複雑でダイナミックなものにしています。

もしお金がなければ、商品やサービスを売買するのはずっと難しくなり、私たちの経済は今ほど発展していなかったでしょう。

クラス演習：次の例は、お金のどの機能を示していますか？

- ◆ エヴァンは子犬を買うために、毎週の給料の一部を貯金することにしました。
- ◆ アダムは、ピザ屋でピザ2切れを1,200円で購入しました。
- ◆ マークは、10,000円のコンサートチケットを買うか、13,000円のスキーパスを買うか迷っています。

2.3 お金の性質

時が経つにつれて、人々は「お金が交換手段としてきちんと機能するためには、特定の性質を備えている必要がある」と気づくようになりました。

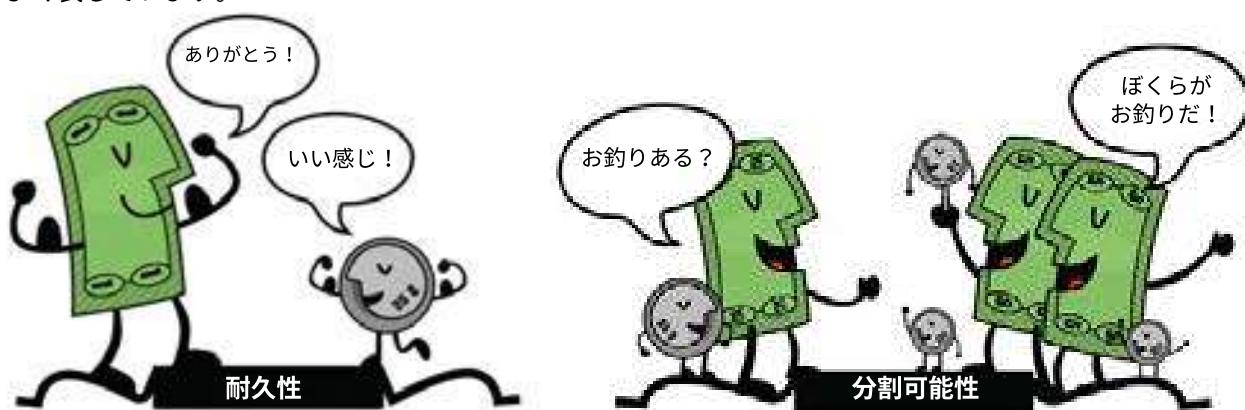
その性質とは、耐久性・分割可能性・携帯性・受容性・希少性・均一性です。

◆ 耐久性とは、お金が物理的に劣化せず、長く使い続けられる性質のことです。
耐久性に優れていれば、お金は傷んだり形を変えたりせずに経済の中で流通し、誰もが受け取れる状態を保てます。

例えば、金（ゴールド）は、摩耗や劣化に強い素材であり、お金の「耐久性」という性質をよく表しています。

◆ 分割可能性とは、お金が小さな単位に分けられる性質のことです。
分割可能性を有していれば、人々はさまざまな金額の買い物ができるようになります。

硬貨は簡単に小さな額面に分けることができ、お金の「分割可能性」を表す例として挙げられます。



お金とは何か？

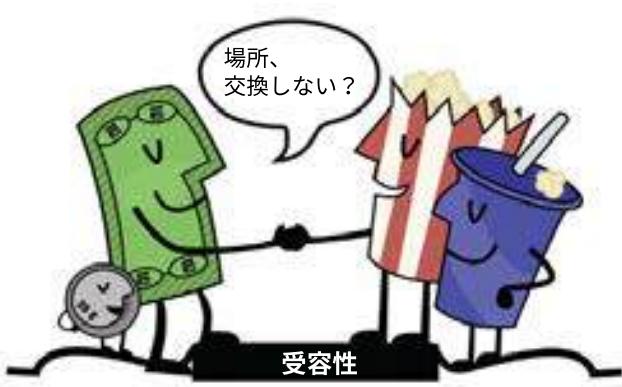
携帯性とは、お金を簡単に持ち運べることを指します。
お金が携帯性を有していれば、人々はお金を持って商品やサービスを不自由なく売買できます。

クレジットカードは財布やカバンに簡単に入れて持ち歩くことができ、お金の携帯性をよく表しています。



受容性とは、支払い手段としてお金が広く受け入れられていることを指し、これにより人々は安心して商品やサービスを売買できます。

米ドルは支払い手段として広く受け入れられている通貨であり、お金の受容性を表す例として挙げられます。



希少性とは、お金の供給量が限られていることです。供給量に限りがあるとお金の価値が保たれ、同じ量の商品を買うのにより多くのお金を使わずに済みます。

収集用切手、特に希少価値の高いものは、時間とともに価値が上昇するため、良い貨幣の形態となる可能性があります。切手収集家は資産を分散する手段の1つとして、切手を使用することもあるのです。



均一性（代替可能性）とは、互換性（別のものと置き換えても問題なく機能する性質）を指します。同じ種類のお金であれば交換可能で、同じ価値として扱われます。

お金は均一であるべきで、例えば10円玉はどれも大きさや重さが均一です。1円玉はいつでもどこでも1円玉として使えます。



第2章

お金のこれらの特徴は、貿易や商取引を促進するための便利で効果的なツールとなり、経済の発展と安定に欠かせません。

クラス演習

さまざまな資産にはそれぞれ異なる特性があり、お金としての機能を異なる程度で果たします。社会は最終的に、安定性・希少性・分割可能性・譲渡性（簡単に他人に渡せるか）・および交換手段としての受容性などの要素をもとに、どの資産をお金として使うかを決めます。

お金の特徴にどのくらい合致するかを判断するために、各特徴について1～5のスコアをつけてみましょう。各項目の合計点を出すことで、どれがお金の形態として最も適しているかを判断します。

[0 = ひどい、 3 = まあまあ、 5 = よい]

※ ビットコインの列は今は記入しないでください。このコースの後半で改めて取り上げます。

次の質問を参考にして、表にあるそれぞれの項目がどれだけ「お金の特徴」に当てはまるかを判断してみましょう。

-  耐久性：時間が経っても摩耗や劣化に耐えられますか？
-  携帯性：簡単に持ち運べて、異なる場所で使えますか？
-  均一性：他の形式のお金と交換できますか？
-  受容性：支払い手段として広く受け入れられていますか？
-  希少性：供給が多すぎず、希少なものですか？
-  分割可能性：小さい単位に分けて使えますか？

良いお金の特徴	 牛	 タバコ	 ダイヤモンド	 ユーロ	 ビットコイン
耐久性					
携帯性					
均一性					
受容性					
希少性					
分割可能性					
合計					

お金とは何か？

2.4 お金の種類

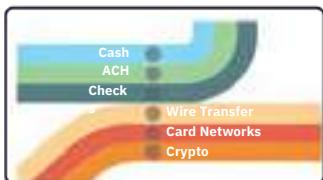
お金は、物理的なお金とデジタルのお金という、2つのカテゴリーに大別できます。

物理的なお金に含まれるもの：

- ◆ 法定通貨：政府によって発行され、交換手段として受け入れられている紙幣や硬貨。
- ◆ 代表貨幣：物理的な商品（コモディティ）に対する請求権を表すお金。
- ◆ 商品貨幣：それ自体に本質的な価値があり、交換手段として広く受け入れられている物理的な物体。
(例：金や銀)

商品貨幣	代表貨幣	法定通貨
 火薬のようなモノが、かつては商品貨幣として使われていたこともあります。		
	銀証書のような代表貨幣は、銀と引き換えることができました。	現在の連邦準備銀行券は法定通貨であり、連邦政府によって債務支払いの手段として認められています。

一方、デジタル通貨はオンライン取引で使えるお金全般を指し、電子通貨・ステーブルコイン・暗号資産などが含まれます。
電子通貨はデジタル版の通常のお金（例えば円やドル）であり、オンラインで商品を売買する際にデジタル決済の仕組みを通じて使われます。



ペイメントレールとは、電子通貨やその他のデジタル資産のある場所から別の場所へ移動させる仕組み（インフラ）のことです。
なお、従来の金融システムでは、銀行やその他の金融機関といった仲介者が常に存在します。
彼らは手数料を取り、取引を承認・キャンセル・取り消し・遅延させる権限を持っています。

代表的なペイメントレールには次のようなものがあります。

カードネットワーク：顧客がデビットカードやクレジットカードで支払いを行う時に、金融機関と加盟店の間での資金移動を仲介する仕組み。

デジタルウォレット：ユーザーが電子通貨を保管・管理し、自分の口座から相手の口座へ送金して支払いを行うオンライン口座。

第2章



中央銀行デジタル通貨（CBDC）

その国の法定通貨のデジタル版で、中央銀行が発行し、政府を介して運用されます。



ステーブルコイン

米ドルなどの資産に対し、安定した価値を維持するように設計されたデジタル通貨です。



暗号資産

デジタル通貨の一種です。ルールに基づいて分散的に管理されているものもあれば、少数の人によって中央集権的に管理されているものもあります。

究極的にいえば、仲介者なしで機能する通貨は通貨供給の支配や権力の集中を防ぐため、社会にとってより効率的で有益です。

しかし、当事者間の信頼に頼らず安全に取引できる通貨をつくることは、歴史を通じて難題でした。それを実現するには、インターネットのように誰にでも分散され、同時に誰にも支配されていない通貨をつくる必要があります。

そのためには、権力を持つ者を含むすべての当事者が、より大きな公益のために支配を手放すことに合意しなければなりません。

2.5 お金の心理学：希少性、時間選好、トレードオフ

砂漠で立ち往生していて、手元に水のボトルが1本しか残っていないと想像してみてください。あなたは喉が渇いていて、今すぐにでも水を飲みたいところですが、同時にこの水は、次に水を見つけるまでの命綱であることも分かっています。

これは「希少性」の典型的な例です。限られた資源（水）しかない中で、それをどう使うかという選択を迫られています。このような状況では、水ができるだけ長持ちするように、少しづつ時間をかけてちびちびと飲むことを選ぶかもしれません。

お金とは何か？

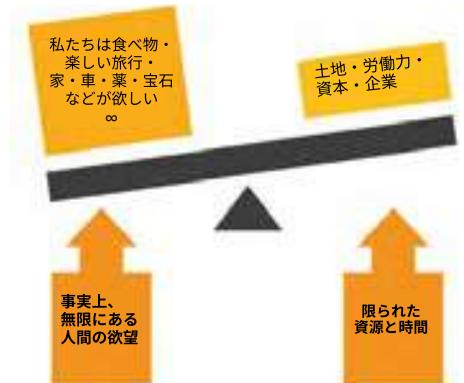


希少性は私たちにとって、限られた資源をどう使うかのメリットとデメリットを比較・検討させ、トレードオフ（何かを得るために何かを諦めること）を迫ります。

あるいは、あなたは水を一気に飲み干して、体を潤わせることで次の水を探すエネルギーを得ようと考えるかもしれません。
どのような選択をするにしても、あなたは困難な決断に直面します。
この場合は「今すぐ喉の渇きを癒すこと」と「後々のために水を温存すること」の間での選択です。

この「希少性」という考え方は、水に限らず、あらゆる資源に当てはまります。
お金や時間、さらには愛情や他人からの注目に至るまで、私たちは常に
「限られた資源をどう使うか」という選択に直面しているのです。

希少性には、人工的なものと自然なものの2種類があります。



- ◆ 人工的な希少性（中央集権的な希少性）は、限定版のデザイナーバッグや、レアなスポーツカード、ナンバリングされたアート作品などを指します。これらは比較的簡単に複製や偽造が可能です。
- ◆ 一方、自然の希少性（分散的な希少性）は、塩や貝殻、金のような貴金属などを指します。
これらは複製や偽造が難しい資源です。
この2つの違いは「管理」にあります。

中央集権的な希少性は、企業や政府のような一つの存在によって管理されますが、分散的な希少性は誰にも管理されません。

中央集権的な希少性の一例として、貧困層に大きな影響を与える「きれいな水へのアクセス」があります。
一部の地域では、この重要な資源が民間企業や政府機関によって管理され、供給の制限や水不足につながっています。
このような中央集権的な管理は、水の価格上昇やアクセスの不平等を招き、結果として貧困層に大きな負担がかかるのです。

きれいな水へのアクセスが制限されることの悪影響は、健康や生活の質が損なわれるだけに留まりません。
水を得るために高いコストを払ったり、長距離を移動させられたりすることで、貧困がさらに悪化するのです。
希少性は私たちの選択に影響を与えます。それを理解することで、より良い意思決定ができるようになります。

自先の利益と将来の利益のどちらを取るかという選択は、私たちの目標達成への道を形作るものなのです。



時間選好とは、「後で得るより今欲しい」と人が感じやすい心理傾向のことです。



第2章

時間選好の例：

例えば、あなたが「今日10,000円を受け取るか、1年後に11,000円を受け取るか」を選べるとします。

時間選好が高い人は、今すぐ10,000円を手に入れることを選ぶかもしれません。

なぜなら、1年待って1,000円多くもらうよりも、「今」10,000円を得ることに価値を感じるからです。

一方、時間選好が低い人は、より大きな報酬を得るために待つことを選びます。

長期的な計画を重視し、自らの欲求にあまりとらわれていないのです。

アクティビティ：時間選好

高い時間選好 vs 低い時間選好

- 1 「キャンディの選択」について、先生から説明を聞きましょう。
- 2 「今すぐ小さなキャンディやマシュマロをもらう」か、「授業の最後まで待って、2個のキャンディ、またはより大きなキャンディをもらう」か、どちらかを選びましょう。
- 3 選択したら先生に伝えてください。
あなたの決定に基づき、すぐにキャンディを受け取るか、授業の最後に受け取るかします。
- 4 活動についてクラスで話し合い、あなたの判断理由や「時間選好」の考え方について振り返りましょう。

まとめとディスカッション：

- ◆ 「今すぐキャンディをもらうか、それとも後でたくさんもらうか」を決める際、あなたの選択に影響を与えた要因は何でしたか？
- ◆ 活動を終え、自分がとった選択について今はどう感じていますか？
- ◆ 「時間選好が高いと不利になり、時間選好が低いと有利になる」という、実生活の具体例を挙げられますか？
- ◆ 高い時間選好ではなく低い時間選好を選んだ場合、どのような結果が生じる可能性があると思いますか？

砂漠を例に当てはめると、喉が渇いているという理由で、今すぐ水を一気に飲み干してしまうかもしれません。将来また喉が渇くかもしれない可能性より、今感じている渴きの方が強く感じられるからです。

一方、水を少しづつ飲んで節約することを選ぶなら、それは時間選好が低いことを示しています。今の渴きを我慢しても、より長く生き延びる可能性を高めようとしているのです。

「機会費用」という概念は、「希少性」と「時間選好」の考え方に関連しています。

お金とは何か？



機会費用とは、ある決断を下す際に諦める「次に良い選択肢」の価値のことです。
すべての決断にはトレードオフが伴います。

今日の選択



900円のストロベリー
スムージーを買う

今



900円を別のことを使う



将来



900円を定期的に貯蓄して得られる恩恵



砂漠の例でいえば、水をすべて一気に飲んでしまうと、水を節約して長い期間使うことで得られる可能性のある、生存上のチャンスを失います。

例えば、水を節約し、時間をかけて少しづつ飲むことを選んだとします。その結果、さらなる水を探すための体力と水分を保つことができました。

そして探している途中、わずかな水分を含んだサボテンを見つけたとしましょう。多くはないものの、一時的に渴きを癒すには十分な量です。

もし最初に水を全部飲んでしまっていたら、サボテンを見つけるための体力すら残っていなかったかもしれません。この場合、一気に水を飲んでしまうことによる機会費用とは、サボテンを見つけて水分を補給するチャンスを失うことです。

この例は、機会費用というのが「選択肢の間にある目先のトレードオフ」だけでなく、選択の結果として「将来に得られるかもしれないチャンス」までも含むことを示しています。

人が「今すぐ小さな報酬を受け取ること」と「将来の大きな報酬を待つこと」のどちらを選ぶかは、時間選好、つまり「目先の満足」と「長期的な計画」のどちらに価値を置いているかによって左右されます。

この章では、お金の基本的な概念について学び、定義・役割・性質・種類について理解を深めました。
また、お金に関する心理的な側面にも触れ、「希少性」「時間選好」「トレードオフ」といった重要な概念を扱いました。

これらの学びは、お金の本質や、私たちの生活における役割を理解するための土台となります。
次の章では、お金の歴史とその進化について見ていきます。

第3章： お金の歴史

3.0 はじめに

アクティビティ：物々交換ゲーム

3.1 物々交換から現代通貨への進化

3.1.1 初期のお金の抱えていた問題

3.1.2 硬貨と紙幣の発展

3.1.3 健全な通貨から不健全な通貨への移行

3.1.4 紙からプラスチックへ

3.2 デジタル通貨

生徒用ワークブック

日本語版 | 2025年版

お金の歴史

3.0 はじめに

お金は最初から計画的に作られたものではなく、市場の中から自然に生まれたものである。政府によって作られたものではなく、時間とともに自発的な秩序として現れたのだ。

マレー・ロスバード



ずっと昔、今のような硬貨や紙幣がなかった時代を想像してみてください。当時の人々は、貝殻や金のような貴金属を「特別な通貨」として使い、物々交換をしていました。一見変わった方法に思えるかもしれません、当時の人々にとっては、それが「みんなが価値を認めたお金」だったのです。

この章では過去にさかのぼりながら、お金がどのように始まり、どんなふうに進化・適応してきたのかを見ていきます。

アクティビティ：物々交換ゲーム

先生から小さな紙が渡されます。あなたの目標は、歴史上の商取引を模したゲームにおいて、その紙に書かれた「持っているもの」を「欲しいもの」に交換することです。紙の一番上には、小さくあなたの名前を書いてください。

★ ラウンド1：物々交換

今は紀元前6000年です。もちろん、現代のようなお金はまだ存在しません。あなたはメソポタミアにて、他の人と商品やサービスを直接交換しています。

補足：現在でも現金を使わずに商品やサービスのやり取りを受け入れている事業者は多く存在します。こうした物々交換による取引も、政府の税務上は通貨による取引と同様に扱われます。

💡 点線に沿って紙を切り離してください。
目標は、「持っているもの」を他の人と何回も交換しながら、最終的に「欲しいもの」を手に入れることです。
※「欲しいもの」は変更できません。このゲームの制限時間は5分です。

第3章



あなたが手に入れた「持っているもの」が「欲しいもの」と一致したら、自分の席に戻ってください。
時間が終わるまでに交換相手が見つからなかった場合も席に戻りましょう。



1回の交換で欲しいものが手に入った人は手を挙げてください。
2回でできた人は？ 3回ではどうですか？

以下の質問に、簡潔かつ具体的に答えてください。

1. なぜ、うまく交換できた人とできなかつた人がいたのでしょうか？

2. 物々交換の利点は何ですか？

3. この活動を体験してみて、物々交換の欠点は何だと思いましたか？

◆ ラウンド2：商品貨幣

時間進めて、紀元前14世紀ごろのアフリカ西海岸に行ってみましょう。物々交換は面倒で非効率になってきました。文明は進化し、この頃は「商品貨幣」を使うようになっていきます。

カウリ貝から硬貨へ



紀元前1300年



紀元前1000年



紀元前687年



豆知識

カウリ貝は、アフリカの一部地域では20世紀まで法定通貨として受け入れられてきました。

紀元前1300年

カウリ貝がアジア・アフリカ・オセアニアのほとんどの地域と、ヨーロッパの一部地域で主要な支払い手段となる。

紀元前1000年

中国の西周王朝が金属硬貨の使用を開始する。

紀元前687年

リディア王（現在のトルコ）のアリュアッテス王が、西洋で初めて金属硬貨の鋳造を命じる。

これらの初期の硬貨は楕円形で、「エレクトラム」（金と銀の合金）でできており、片面のみに模様が施されていました。

お金の歴史

先生からマカロニを1つ渡されました。ここでは単純に、すべての商品の価格をマカロニ1つと仮定します。

あなたの目標は再び「欲しいもの」を手に入れることです。

しかし今、人々は少し賢くなり、いくつかの問題を解決する方法を見つけました。

- ◆ なぜマカロニが商品貨幣とみなされるのでしょうか？
 - ◆ マカロニを使い、どのようにして欲しいものを手に入れていますか？
 - ◆ マカロニを使う方が、物々交換より簡単でしたか？
 - ◆ なぜお金が商品に取って代わったと思いますか？
 - ◆ 商品貨幣を使うことは、物々交換と比べてどのように効率的ですか？
 - ◆ マカロニをお金として使うことにはどんな欠点がありますか？
 - ◆ スペインが船いっぱいのマカロニをあなたのコミュニティに持ち込み始めた時、何が起きたと思いますか？
(アメリカ大陸の金や銀がスペインに持ち込まれたように！)
-
-
-

3.1 物々交換から現代通貨への進化

3.1.1 初期のお金が抱えていた問題



「紙幣の歴史 (The History of Paper Money)」シリーズの中から、
「交換の起源 (Origins of Exchange)」という短い動画を
見て学ぼう。

物々交換経済では、人々は自分が持っている財やサービスの相対的な価値に基づいて、互いに取引します。

こうした経済は非効率的で、特に複雑な社会では管理が困難です。

物々交換の仕組みでは、「欲求の二重の一致」といえるような状況が必要です。つまり、自分が欲しいものを持っているだけでなく、自分が提供したいものを欲しがっている相手を見つけなければなりません。

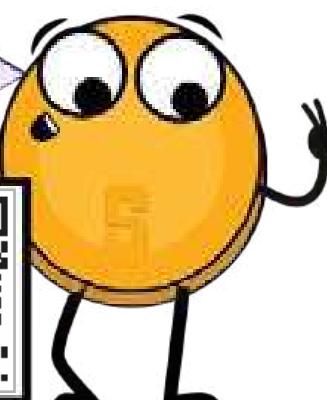
第3章



こんな状況を想像してみましょう：

- ジョセフは自分のバナナをヤエルのココナッツと交換したいと思っています。
- しかしヤエルは、自分のココナッツをタミーのマンゴーとしか交換したくありません。
- そしてタミーは、自分のマンゴーをジョセフのバナナとしか交換したくありません。
- 彼らは「欲求の二重の一一致」がないまま、果物交換の無限ループに陥ってしまいました。
- ジョセフは「冷たいソーダと果物を交換すればいいじゃないか」と提案しますが、彼らは自分たちが孤島にいて、ソーダなど存在しないことに気づきます。
- 結局、3人はビーチに座って、黙ってそれぞれの果物を楽しむことにしました。

この動画は
「紙幣の歴史」
シリーズの第2話
「ヌードルだけじゃない (Not Just Noodles)」だよ。



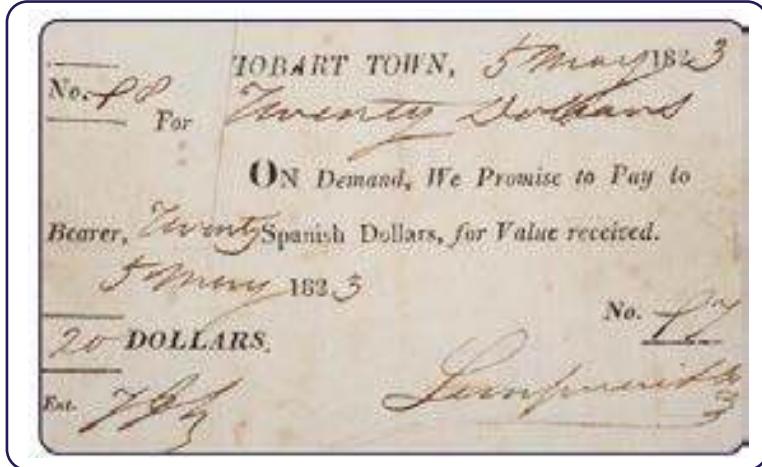
3.1.2 硬貨と紙幣の発展

あなたとあなたのコミュニティが貿易・商業に深く関わるようになるにつれて、物々交換やその他の非貨幣的な交換手段には限界があると気づきます。
そして、貨幣として金属硬貨を採用することを決めました。



商品貨幣とは、金や銀などの価値ある金属素材で作られたお金のことです。
これらは歴史的に「価値の保存手段」「交換の媒介」として、さらに古くは「価値の尺度（記帳単位）」として使われてきました。

お金の歴史



しかし、金属硬貨を頻繁に使うようになると、いくつかの欠点が出てきました。
硬貨は重く、大量の取引には持ち運びが不便です。

また、一部の人々は仕組みを悪用し、
硬貨を溶かして安価な金属と混ぜ、新しい硬貨を作り出していました。
これは物価を上昇させ、通貨システムへの信頼を損ねる原因となります。

この問題に対処するため、あなたとコミュニティは「紙の引換書」をお金として使い始めました。

紙幣の起源は古代中国にあります。これらの紙の引換書は、便利で簡単に交換できる通貨の形態であり、金などの貴金属に裏付けられていて、それらと引き換えることができます（17世紀から19世紀にかけては実際にそうされていました）。

この仕組みにより、貴金属の価値と安全性を保ちつつ、より持ち運びや交換がしやすい通貨が実現しました。



3.1.3 健全な通貨から不健全な通貨への移行

時代は17世紀のスウェーデンに進みます。
この頃になると、あなたは貴重な資産を保管する
ために、銀行に完全に依存するようになりました。

しかし銀行家たちの行動には不審な点が見えて
きます。
彼らは保有している金の量以上に紙の引換証を
発行し、裏付けとなる資産以上の貨幣を発行して
いたのです。

このずる賢いやり方で、銀行家は紙の引換証の
価値と、顧客のために保有している金の価値との
差額から利益を得ていました。



紙幣の理論を実際に導入
すると、一体何が起こる
んだろう？
「紙幣の歴史 (The
History of Paper
Money)」の第4話で
確かめてみよう。



第3章

この出来事が、お金の仕組みにおける大きな転換点だと気づくでしょう。

貴金属に裏付けられた「健全な通貨」のシステムから、

モノ的な裏付けを持たない「不健全な通貨（法定通貨）」のシステムへと移行しようとしているのです。

この移行は一夜にして起きたわけではなく、いくつかの要因によって徐々に進んでいきました。

大量生産と都市化を伴う産業革命がその一因となり、銀行や株式市場などの高度な金融システムの発展も影響しました。

中央銀行やその他の金融当局の登場によって、通貨の中央集権的な管理が進み、経済成長を支える手段として法定通貨が発行されるようになったのです。



しかし、この中央集権化には、無責任な消費・負債の増加・経済的なインセンティブ（動機付け）を通じた市民のコントロールなど、負の側面もあることに気づき始めます。

第一次世界大戦までは、紙幣を一定量の金と引き換えることができました。

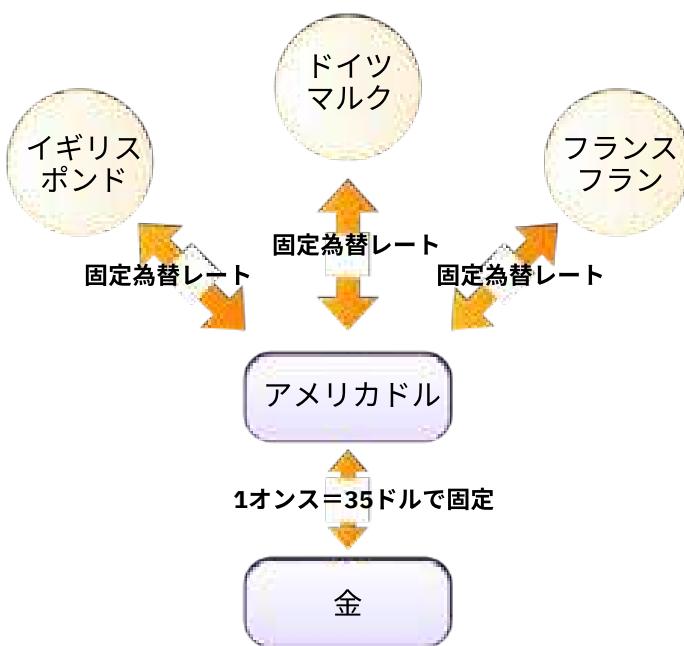
しかし、二度の世界大戦と1929年の世界恐慌によって、その仕組みは終わりを迎えます。

1944年にはブレトン・ウッズ協定が締結され、米ドルが世界の基軸通貨となり、米ドルの価値は金1オンスあたり35ドルのレートで固定されました。

他国の通貨はドルに連動して為替レートが固定され、国際金融市场の安定が図られました。

ブレトン・ウッズ体制

(1945-1972)



残念ながら、このシステムは1960年代後半から崩れ始め、1971年のニクソン・ショックへとつながりました。

アメリカ政府はドルの金への兌換を停止したのです。

これにより金本位制は終わりを迎え、世界は「借金の創出と蓄積」によって動く時代へと突入します。

日常生活を送る中で、あなたはお金の価値が以前ほど安定していないことに気づき始めます。

柔らかい定規でテーブルの長さを正確に測るのが難しいように、通貨の価値が権力者の気まぐれに左右される世界では、モノやサービスの価値を正確に測るのは困難です。

金のような、いかなる実物資産に裏付けられていないお金の価値に慣れることに、混乱と不安を感じ始めるでしょう。

お金の歴史

この変化が世界経済に与える影響を目の当たりにし、あなたは法定通貨の安定性や信頼性に疑問を抱き始めます。

現代の世界では、ドルは金に裏付けられていた頃のように固定された安定的なものではなく、変動の影響を受ける通貨となったことに気づきます。

ドルの価値はインフレ（物価上昇）・金利・国の経済力・政治的イベント・市場投機・国際貿易の需要など、さまざまな要因に影響され、計算単位として使うのが難しくなります。

変動し続けるドルの価値に翻弄されながら日常生活を送る中で、混乱や先の見えない不安に直面するのです。

現代の金融システム・効率性の向上・情報へのアクセス拡大・コミュニケーションの強化を通じて、生活の質を向上しようと努力したにもかかわらず、大多数の人々の生活水準は以下のような理由で低下し始めます。

- ◆ 中央集権の乱用
- ◆ 物価の上昇
- ◆ 実質賃金の停滞
- ◆ 通貨の弱体化
- ◆ より少ないモノを得るために、より多くのお金を支払わなければならない状況

こうした状況は、教育・信用・資源・社会的ネットワーク・政治的代表へのアクセスといった面で制約のある、経済的に恵まれない人々にとって大きな困難をもたらします。

彼らは成功するために必要な要素へのアクセスが限られているため、不利な立場に置かれてしまうのです。

その結果、富裕層はますます豊かになり、貧困層はますます貧しくなる傾向にあります。



3.1.4 紙からプラスチックへ

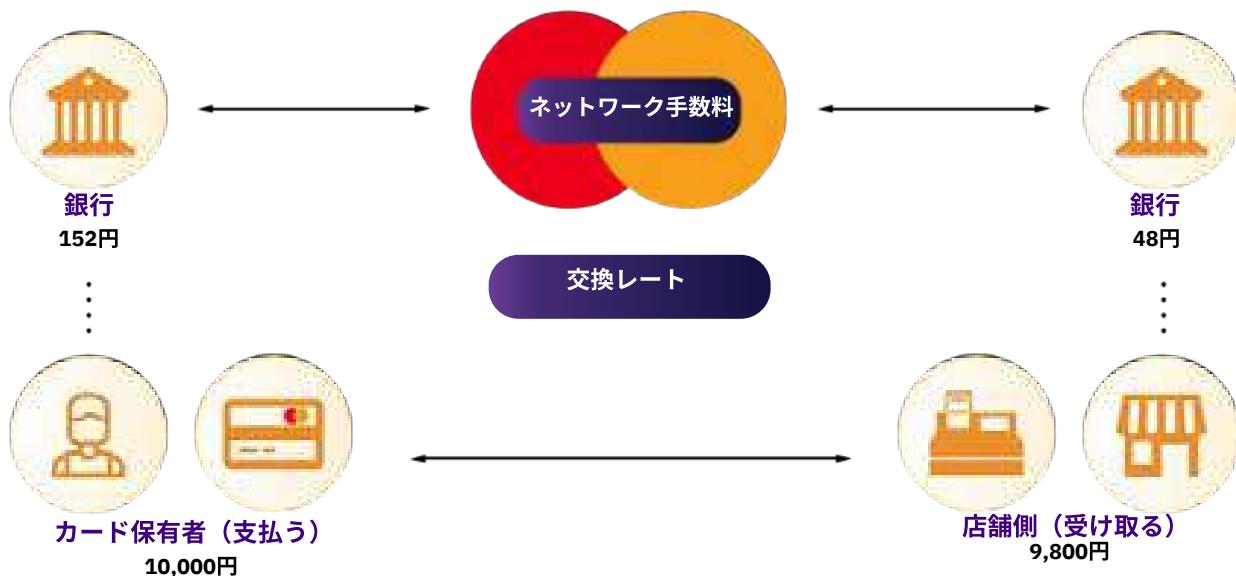
1950年代に最初のクレジットカードが登場して以来、ずいぶん進歩しました。

プラスチック製のカードをかざすだけで、いつでも好きな物を手間なく買えます。

まるで無限の可能性が広がる世界への扉が開かれたようで、その先に何が待っているのかというワクワク感に満ちていました……そう、当時はそう思っていたのです。

ところが、クレジット（信用取引）への依存には、物価上昇や破綻を招く経済構造を助長するような深刻な後遺症があることに、当時は誰も気づいていませんでした。

第3章



テクノロジーの進化に伴い、お金の取り扱い方も変化しています。
インターネットは金融の世界で主要な役割を果たすようになり、ネットバンキングやECサイトによって、
お金の管理や支払いをすべてオンラインで行えるようになりました。

デジタル通貨の台頭は、こうした進化の中で次なる大きな一歩となり、新たな可能性を広げ、
金融取引のあり方を変えつつあります。

3.2 デジタル通貨

デジタル通貨は従来のお金とは異なり、電子的な形でのみ存在する通貨です。
コンピューターや専用のソフトウェアを使って保存・送受信されます。
デジタル通貨を使えば、インターネットを通じて個人がお金を送れます。
Eメールが送料なしでメッセージを瞬時に届けられるのと同じように、デジタル通貨も即時かつ非常に低コストで
お金の価値の送受信が可能です。

私たちが現在使っている通貨も、どんどんデジタル化が進んでいます。
貨幣供給量のうち、硬貨や紙幣の形で存在する割合はほんの一握にすぎません。
銀行や金融サービスは、インターネットを通じて簡単に送金や決済ができるアプリを提供しています。

しかし、そのお金はいったいどこから来ているのでしょうか？

この章では、金に代表される健全な通貨から、紙の形をした不健全な通貨、そしてデジタル化された
法定通貨へと移り変わる様子を見てきました。
次の章では、現在の法定通貨制度がどのように機能しているのか、どのようにして誕生したのかを探ります。

第4章： 法定通貨とは 何か？ 誰が管理している？

4.0 はじめに

4.1 法定通貨の簡単な歴史

4.2 法定通貨システム

4.2.1 法令によって成り立つ金融システム

4.2.2 部分準備銀行制度：負債によって支えられる仕組み

アクティビティ：部分準備銀行制度

4.2.3 誰が法定通貨システムを管理していて、どのような利益を得ているのか？

4.3 中央銀行デジタル通貨（CBDC）：法定通貨の未来

生徒用ワークブック

日本語版 | 2025年版

法定通貨とは何か？誰が管理している？

4.0 はじめに

人類の歴史は、お金が価値を失っていく歴史である。

ミルトン・フリードマン

前章では、お金がどのように進化し、貨幣システムが「健全な通貨」から「不健全な通貨」へと移行し、現在の世界を形成してきた過程を見てきました。

この章では、これらの変化が現在の法定通貨制度にどのようにつながったのか、そしてその法定通貨制度がどのように機能しているのかを深く掘り下げます。

現在の法定通貨制度はどのようなものなので、どのようにして誕生したのでしょうか？

この問い合わせるには、まず世界の現在の基軸通貨であり、今日の世界で支配的な役割を果たす米ドルに焦点を当てる必要があります。すべての国が、直接的または間接的に、米ドルに関わる影響を受けています。

各国の法定通貨制度を正しく理解するためには、法定通貨制度の発祥地であるアメリカと結びつく、歴史的背景を解き明かすことが不可欠です。

4.1 法定通貨の簡単な歴史

1815-1933	1913	1933	1934	1944	1971	1980
金本位制	中央銀行「連邦準備制度(FRB)」の設立	大統領令6102号によりすべての市民が金を1オンス20.67ドルの交換レートで引き渡す義務を負った。	ゴールド・リザーブ法。金1オンスあたり35ドルへと40%切り下げることで、実質的に国民から富を奪った。	ブレトンウッズ協定により、米ドルが世界の主要な基軸通貨になる。	ニクソン・ショック。米ドルの金への兌換が終了し、法定通貨制度が誕生。	金の価格が1970年の1オンスあたり35ドルから、1980年には1オンスあたり870ドルに上昇。人々の貨幣価値がわずか10年間で96%失われた。

時系列

19世紀には、世界中の文明が「健全な通貨」基準に基づいて栄え、金や銀のような希少性・耐久性・認識性のある貴金属が使われていました。

世界貿易の拡大に伴い、大量の金属の持ち運びが困難になり、金や銀を保管する倉庫が登場します。

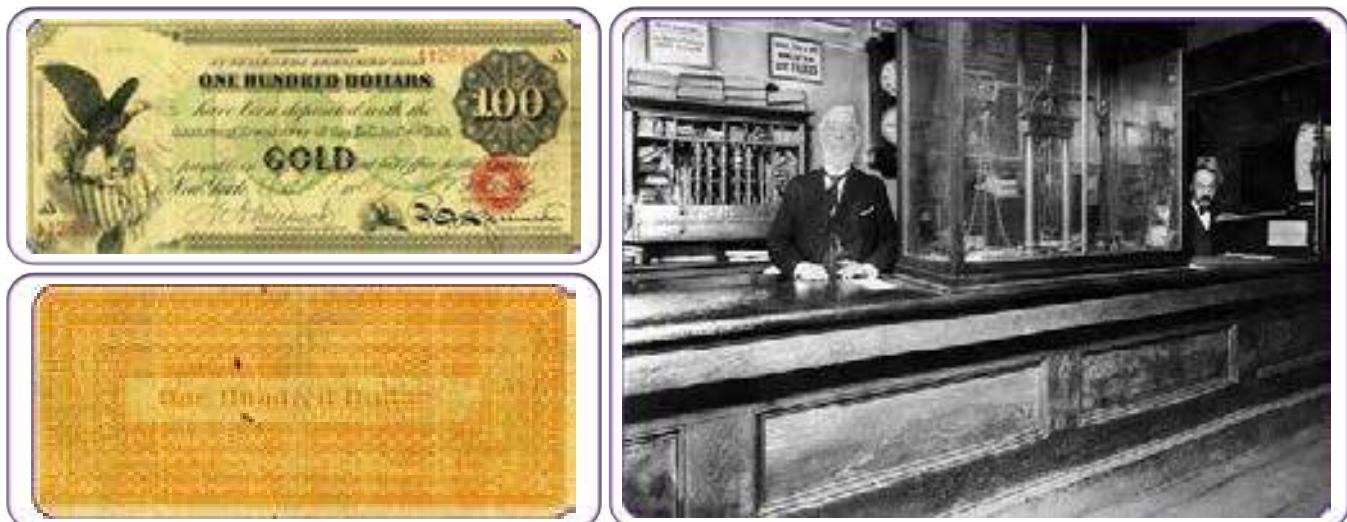
これらの倉庫は人々の貴金属を安全に保管し、特定の量の金や銀と引き換えできる紙の証書を発行していました。

人々は貴金属を預ける代わりに、紙の証明書を受け取っていたのです。



第4章

それらの証書は、預けた金や銀の量と正確にひもづけられていました。
この「紙と実物資産が直結した仕組み」こそが、現在私たちが知っている「銀行」のはじまりだったのです。



元々、銀行は顧客の資産を安全に保管するのが目的でしたが、次第に保有していない金に対しても証書を発行するという、リスクの高い貸出業務に乗り出すようになります。このような行為は、預金者が一斉に資産の返還を求めた場合、取り付け騒ぎにつながる危険性がありました。

このリスクに対処するため、銀行は政府と協力して再貸出を合法化する仕組みを整えました。

そして1913年には、新たな紙の証明書を発行し、経営難に陥った銀行を救済する役割を担う中央銀行として、連邦準備制度（FRB）を創設したのです。

各国の政府は金や銀の価値を認識していたため、その管理をめぐる紛争や戦争につながりました。

第二次世界大戦に至るまでの数年間、レーニン、スターリン、チャーチル、ルーズベルト、ムッソリーニ、ヒトラーといった指導者たちが、戦略のために金を押収していました。

1930年代初頭、アメリカでは「お金の裏付けとなる資産」のあり方に大きな変化が起こります。

当時、多くの人々の財産は金の形で保管されていました。ところが1933年、ルーズベルト大統領は「大統領令6102号」を発令し、すべての市民に金を差し出すよう命じたのです。

これは自発的な交換ではなく、拒否すれば重い罰則が科される強制的な命令でした。

政府は交換レートを金1オンスあたり20.67ドルに設定しました。これは、1オンスの金に対して、20.67ドル相当の紙の証明書を受け取ることを意味します。

人々はこの紙幣を受け取るしかなく、「いつかまた金と交換できるかもしれない」と願うしかなかったのです。



法定通貨とは何か？誰が管理している？

1934年、ゴールド・リザーブ法によって、人々は再び紙幣を金と交換できるようになりました。

しかし、そこには落とし穴がありました。

政府は交換レートを金1オンスあたり35ドルに引き上げることで、意図的に紙幣の価値を切り下げたのです。

この切り下げは、特に低・中所得層の勤労者に大きな打撃を与えました。

それまでの貯金の価値が目減りし、実質的に持っていたお金の価値が下がってしまったからです。

第二次世界大戦後、1944年のブレトン・ウッズ協定によって、米ドルが世界の基軸通貨として金と交換できることになりました。

しかしこの金と米ドルのつながりは、1971年にニクソン大統領が金との兌換を停止したことで断ち切られます。

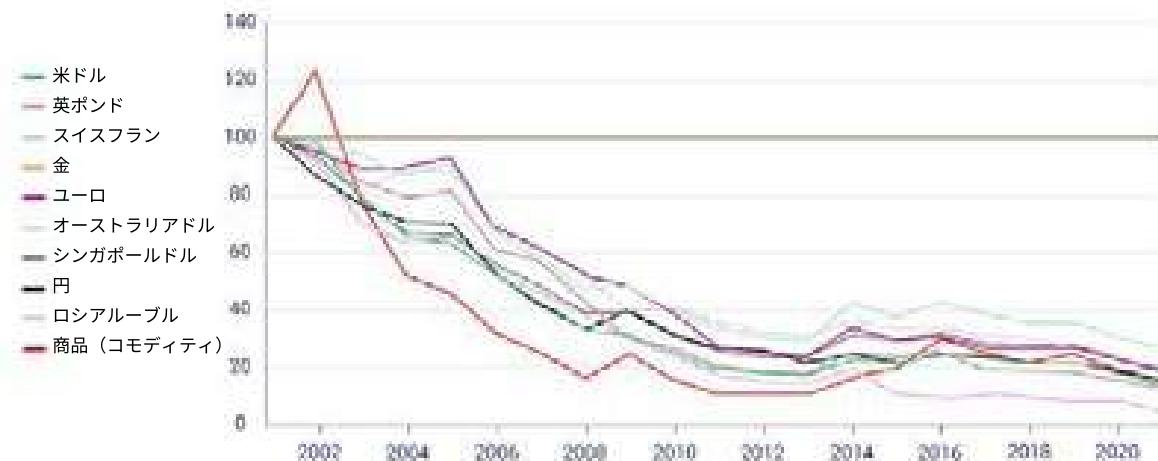
これは非常に大きな転換点であり、金などの物理的な資産に裏打ちされない「不換紙幣制度」への移行を意味しました。

この制度では、通貨の価値はそれを使う人々の「信頼」と「信用」によって支えられることになります。

政府と中央銀行が人々から金を回収し、そのほとんどを保有していたため、

金の価値は高騰して1980年には1オンスあたり870ドルに達しました。

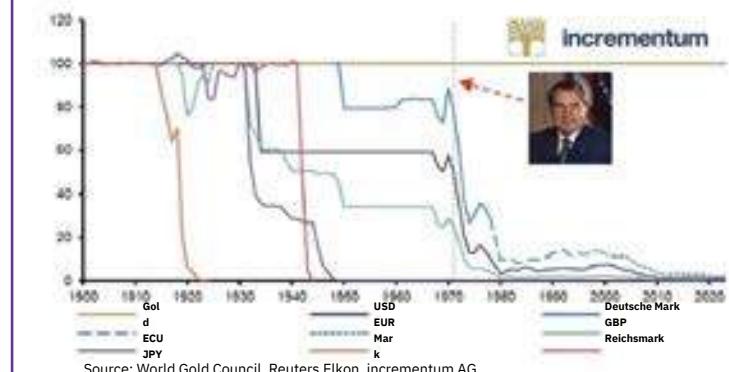
米ドル/金、オンス単位での価値



結論として、人類社会が健全な通貨基準から不健全な（不換紙幣）基準へと移行した歴史は、政府と銀行がいかにして市民から貴金属を奪っていったかを物語っています。

本物の貨幣は政府と銀行の手に渡り、人々の手元には、政府が「これが通貨だ」と定めただけの紙切れが残されたのです。

金と様々な通貨の金換算値、1900年～2023年



第4章

4.2 法定通貨システム

一般的な通貨の根本的な問題は、その仕組みが成立するためにあらゆる「信頼」を必要とする点だ。
中央銀行は通貨の価値を下げないと信じなければならないが、
法定通貨の歴史はその信頼を裏切る事例で満ちている。

サトシ・ナカモト

人類は、多くの人々に管理されていた「健全な通貨」から、少数の人々に管理される「不健全な通貨」へと移行しました。では、この仕組みは実際にどう機能しているのでしょうか？

4.2.1 法令によって成り立つ金融システム

法定通貨システムの特徴は、法定通貨に関する法律を通じて人々に課される強制的な性質です。
「フィアット (fiat)」という言葉はラテン語で「命令によって」という意味があり、当局によって発せられた命令を表しています。

金などの実物資産に裏付けられたお金とは異なり、法定通貨にはそのような裏付けがありません。
代わりに、その使用は法律によって義務付けられているのです。
円・ドル・ユーロ・ポンド・人民元・ペソなど、日常的に使われている通貨はすべて法定通貨に分類されます。

法定通貨に関する法律：
すべての国民に対して、特定の通貨を受け入れることを義務付ける法律。



法定通貨の価値は、「それが商品やサービスと交換できる」という人々の信念と、「時間が経ってもその価値が保たれるだろう」という幻想に支えられています。
例えるなら、法定通貨はコンサートのチケットのようなものです。価値があるのは紙のチケットそのものではなく、バンド（政府と中央銀行）が素晴らしいショー（経済の安定）を見せてくれるという信頼に基づいています。

法定通貨のメリット

- ◆ 使いやすさ：日常の取引に便利。
- ◆ 低コスト・低リスク：金のように厳重なセキュリティを必要とせず、安価で安全。

法定通貨のデメリット

- ◆ インフレのリスク：物価が継続的に上昇し、インフレや歴史的なハイパーインフレを引き起こす可能性がある。
- ◆ 中央集権的な管理と操作：少数の人間がシステムを操作し、検閲や没収を引き起こす可能性がある。
- ◆ カウンターパーティリスク：政府が危機に陥ると通貨の価値が下がることがある。
- ◆ 濫用の可能性：制度が悪用され、汚職や信頼の喪失につながるおそれがある。

法定通貨とは何か？誰が管理している？

コモディティ（商品）と法定通貨：その違いをイメージしよう

おさらい：

法定通貨が登場する前は、政府は金や銀のような、価値があり希少で手に入りにくい実物資産から硬貨を鋳造していました。または、希少な実物資産と交換できる紙幣を発行していました。
これがコモディティ（商品）に裏付けられた通貨システムです。

一方、現在の法定通貨システムは、モノポリー上のお金のようなものです。法定通貨は中央銀行が印刷した紙切れであり、その価値は政府の政策に直接左右されます。
政府や中央銀行は、いわば「モノポリーの銀行役」であり、ゲームのルール・誰が何を得るか・得られるものにどれくらいの価値があるかをコントロールしています。
言い換えれば、政府は通貨システムをうまく管理すると約束しているわけです。

つまり、法定通貨は政府が使用を義務付けているからこそ価値を持つのであり、
法定通貨自体には何の効用もありません。

まとめると、法定通貨システムは信頼のゲームであり、私たちのお金の価値は支配者の約束にかかっているのです。人々は、政府が国民全体の利益のために行動してくれることを願うしかありません。
次に、銀行がどのように新しいお金を生み出すのか、誰が関与しているのか、そしてそれが経済にどんな影響を与えるのかを見ていきましょう。

4.2.2 部分準備銀行制度：負債によって支えられる仕組み

国民が銀行や通貨制度を理解していないのは、とても良いことだ。
もし理解てしまえば、明日の朝までに革命が起きてしまうだろう。

ヘンリー・フォード

部分準備銀行制度は、法定通貨システムの主要な構成要素のひとつです。
この制度では、銀行が顧客から預かったお金の大部分を貸し出すことを可能にしています。
銀行が多くサービスを提供するのはなぜだろう、と不思議に思ったことはありませんか？
一見すると親切に見えるかもしれません、銀行も企業であり、主な目的は利益を上げることです。
では、銀行は人にお金を貸して、どうやって利益を上げているのでしょうか？

銀行は預金に対する利息を得るだけでなく、次のような方法でも収益を得ています。

- ✿ 貸し出したローンに利息を課す
- ✿ ATM利用や口座維持などのサービス手数料を取る
- ✿ 証券の売買や不動産投資などで収益を上げる
- ✿ 貸付金の一部を準備金として保有し、残りを運用や貸付に回す
- ✿ 預金に利息を支払いながら、当座・貯蓄口座に手数料を課す

銀行が預金を受け取った際は、その一部（準備預金）だけを保有し、残りを貸し出しが認められています。



銀行は預金者から
利息で借り入れをする。
(例: 5%)

銀行はこのお金を借り手に
より高い利息で貸し出す。
(例: 9%)



銀行は貸付によって得た利息から、
預金者への利息を支払い
(9% - 5% = 4%)、
差額を利益として得る。

第4章

例えば、あなたが10,000円を預けて預金準備率が10%だった場合、銀行は1,000円だけを準備金として残し、残りの9,000円を貸し出すことができます。

借り手はその9,000円を別の銀行に預けることで、このサイクルは繰り返されていきます。

最初は10,000円の預金から始まつたにもかかわらず、経済全体に存在するお金は27,100円にまで増加します。まるで何もないところからお金が生まれたかのように見える、いわゆる「乗数効果」として知られる現象です。

このプロセスは、銀行が貸し出しのたびに新たな通貨を生み出し、全体的な通貨供給量を増加させるため、借金に支えられる金融システムにつながります。

部分準備銀行制度が続くにつれて、経済全体の負債は増え、インフレの一因となるのです。

このシステムは、貸し出しによる通貨創造の連鎖に依存しており、例えるなら薬物中毒者に継続的に薬を与え続けるような状態です。

しかし、銀行が準備金以上にお金を貸し出し、預金者が一斉に引き出しに殺到した場合、銀行は破綻する可能性があります。

こうした事態には、中央銀行が「最後の貸し手」として介入し、銀行の破綻を防ぐために新たな通貨を供給します。

中央銀行はこれを、資産を買い戻したり、銀行口座に直接通貨を注入したりすることで実現します。
要するに、中央銀行が継続的に通貨を注入することで、銀行は破綻から救われるのです。

このような負債に支えられ、中央銀行により常に救済されるシステムは、好況と不況を繰り返す経済サイクルを生み出す一因となっています。

例えば、あなたに銀行家の友人がいるとしましょう。彼の名前はダックスとします。

ダックスは自転車が大好きで、「あちこちに行きたいからあなたの自転車を貸してほしい」と言います。

あなたが彼に自転車を貸すと、驚くことにダックスはその自転車を貸し出すことを、他のたくさんの友人にも同時に約束し始めます。

あなたが貸した1台の本物の自転車を使って、ダックスは架空の自転車をいくつも作り出し、それを友人たちに貸し始めたのです。友人たちはみな、好きなときに快適なサイクリングができると思っています。

しかし現実には、本物の自転車は1台しかありません。他はすべて想像上のもの、つまり単なる約束なのです。

さて、どうなるでしょうか？架空の自転車がたくさん出回り、最初はみんながとても幸せです。

なぜなら、最初のうちは誰も同時に自転車を使おうとしないので、問題はないように見え、みんなに十分な数の自転車があるようを感じられるからです。友人たちは自転車でどこへ行こうかと考えながら、多くの計画を立て始めます。

しかし、ここで魔法が色あせ始めます。

ある晴れた日、みんなが「今日はサイクリング日和だ」と思い立ちます。彼らは全員、ダックスの家の玄関先に集まり、架空の自転車に乗れる楽しみでいっぱいです。

しかし、彼らは厳しい現実に直面します——本物の自転車は1台しかないのです！

がっかりした気持ちが広がり、「自転車に乗れる」という約束の価値は一気に下がります。

部分準備貸付の世界でも、これと似た話が起こります。

銀行は実際に持っている以上のお金を貸し出しており、しばらくの間はみんながその恩恵を受けます。よりお金が多く出回り、どこにでも豊かさがあるように見えるのです。

しかし、多くの人が同時に自分のお金を引き出そうとすれば、現実が明らかになります。

すべての約束を守るのに十分な量のお金がないのです。

このようなシナリオは、関わるすべての人の公共の利益や価値に影響を与えます。

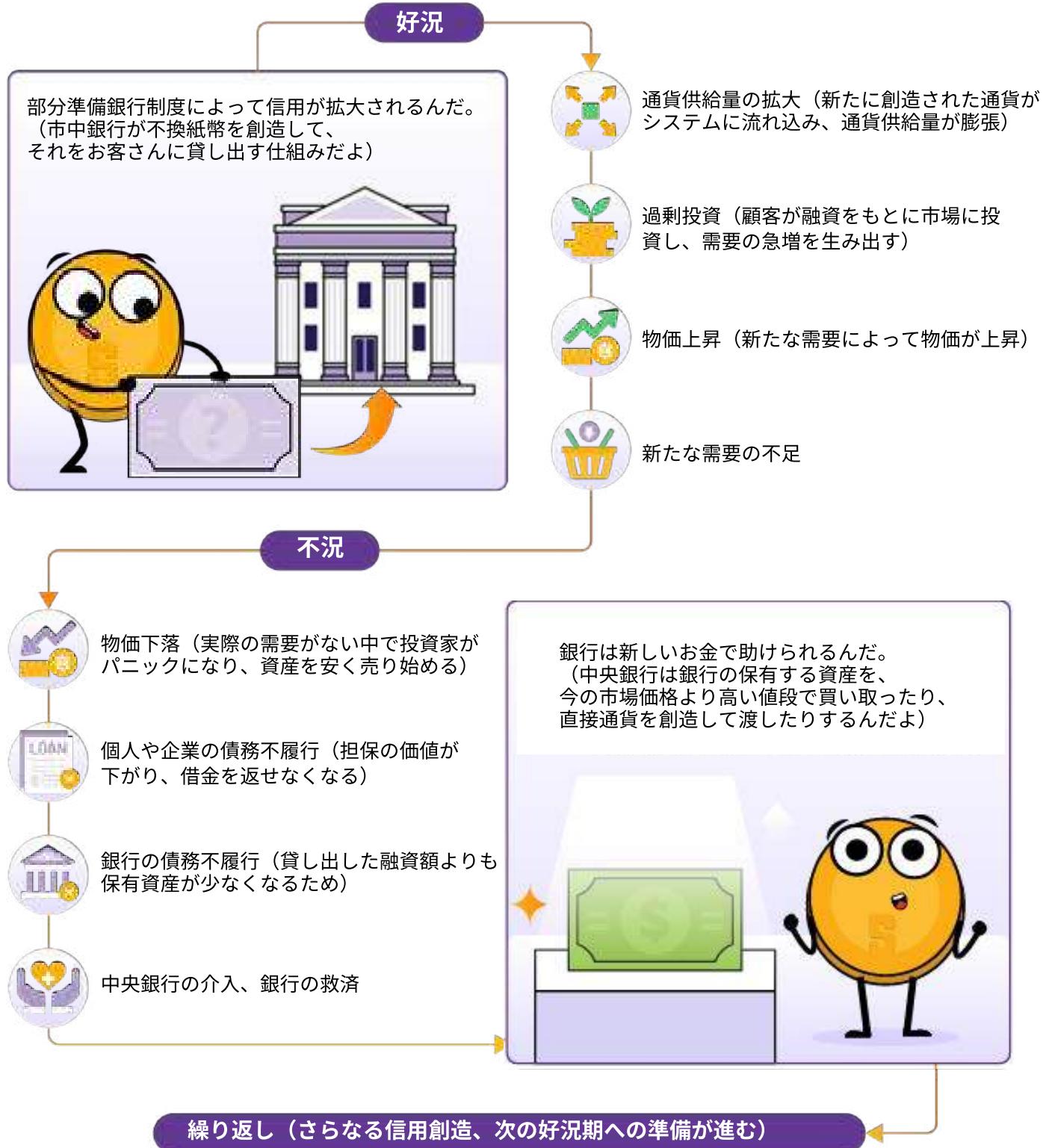
豊かさの約束は、やがて詐欺へと変わっていきます。

みんなが一斉に本物の自転車に乗ろうとしたとき、架空の自転車の価値がなくなったように、みんなが自分の本当の取り分を求めて殺到すると、経済におけるお金の価値が減少する可能性があるのです。

そうなると人々は、銀行にあると思っていたお金は実はそこにはないと気づきます。そして、パニックや取り付け騒ぎ、さらには経済全体の崩壊にまで発展する可能性があります。

これらの崩壊の代償をずっと支払わされてきたのは、世界中の低所得層と中間層の人々なのです。

法定通貨とは何か？誰が管理している？



第4章



アクティビティ：部分準備銀行制度

この演習では、部分準備銀行制度がどのようにして通貨の価値下落、インフレ、購買力の低下を引き起こすかを探ります。

今回は広く使われている準備率10%を用いて、6人の登場人物（うち1人が銀行役）によるシンプルな例で見ていきましょう。

- Aさんは宝くじで1000万円を当てて、それをB銀行に預けます。準備率は10%なので、B銀行は100万円を金庫に残し、残りの900万円を貸し出せます。
 - CさんはB銀行から最大限の900万円を借り、それを使ってDさんから家を購入します。
 - DさんはCさんから受け取った900万円をB銀行に預けます。これで銀行の合計預金額は1900万円になります。
 - EさんがB銀行に融資を申し込み、B銀行は新たな預金の90%である810万円を貸し出します。
 - Eさんはその810万円でFさんから美術品を購入し、Fさんはそのお金をB銀行に預けます。これで銀行の合計預金額は2710万円です。

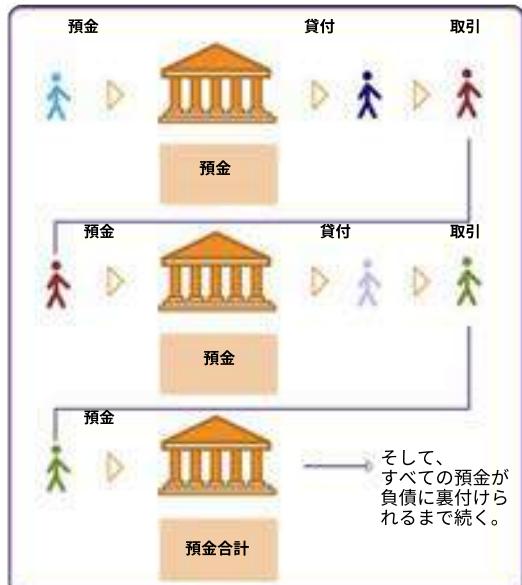
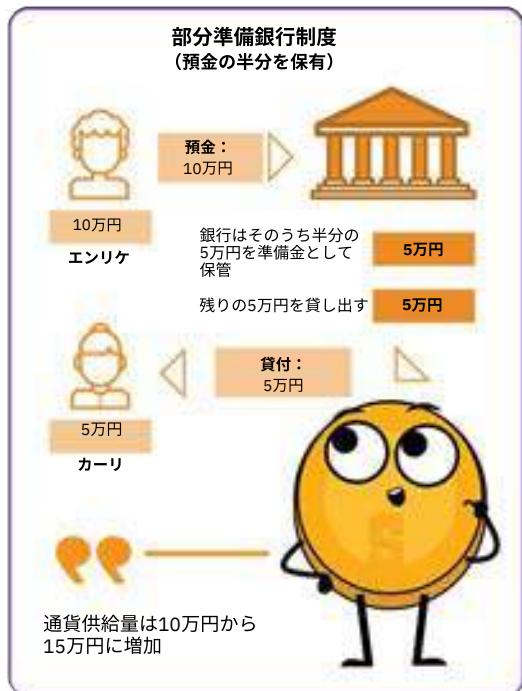
このシナリオでは、最初の1000万円の預金が経済を循環した結果、合計2710万円の預金が生み出されました。もし準備率が1%に引き下げられたら、創造される通貨の量は大幅に増加します ($1000\text{万円} \div 0.01 = 10\text{億円}$)。

この通貨が経済の中でさらに循環し続けた場合、
実際にはどれくらいのお金が創造されることになるでしょうか？

重要なのは、2020年以降、アメリカの中央銀行（FRB）が経済を刺激する目的で、準備率を0%に引き下げたという点です。

必要な役割：

- A = 預金者** (宝くじの当選者) (水色)
B = 銀行の窓口係 (銀行)
C = 債務者1 (濃い青)
D = 不動産所有者／預金者 (赤)
E = 債務者2 (薄紫)
F = 画廊オーナー／預金者 (緑)



法定通貨とは何か？誰が管理している？

4.2.3 誰が法定通貨システムを管理していて、どのような利益を得ているのか？

法定通貨システムを支配し、利益を得ている主要なプレイヤーは、政府・富裕層・金融セクター・中央銀行の4つです。

政府：政府は法定通貨ショーの「演出家」のような存在です。税金の徴収に加え、財務省が発行する新たな負債（国債）によって資金を調達します。これらの国債に十分な需要がないときは、中央銀行がその残りを買い取ります。

つまり政府は、国民の承認を得ずに活動を続け、自分たちの利益を追求できるのです。まるで、返済の心配をせずにクレジットカードを手に入れたようなものです。

政府にとっては都合が良いかもしれません、その代償は他の人々が払うことになります。

富裕層：富裕層は法定通貨システムから大きな恩恵を受けています。より多くの負債を利用できるため、コモディティ・不動産・株式といった資産に投資でき、ほとんど労力なく新たな富を生み出せます。

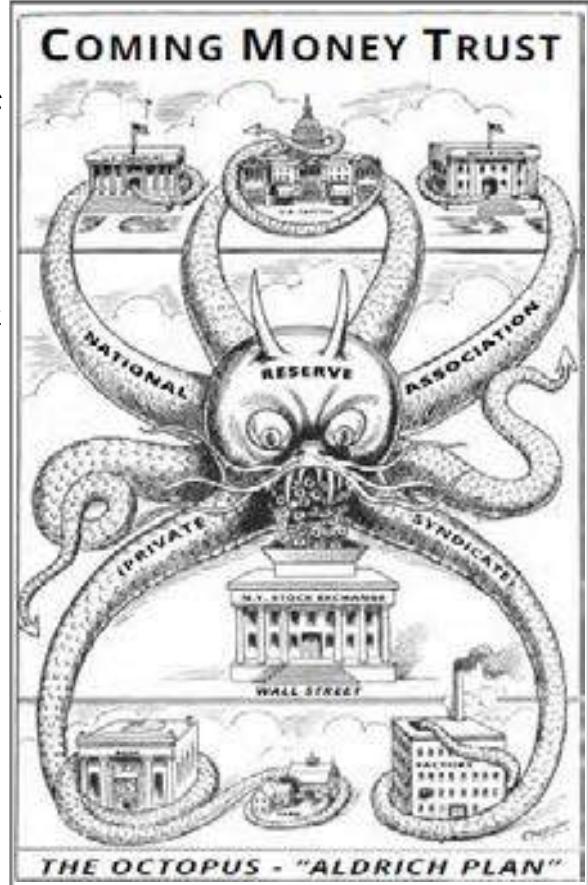
金融セクター（銀行）：銀行やその他の金融機関は、法定通貨システムを直接管理しているわけではありませんが、そこから大きな恩恵を受けています。説明責任から解放されているため、部分準備貸付を通じて新たな通貨の創造を加速させ、より多くの収益を得られます。そしてシステム崩壊を防ぐために新たな不換紙幣で救済されるので、銀行は事実上、何の報いも受けません。

中央銀行：中央銀行は貨幣供給量の増加を管理する、糸を引く存在です。しかしここにはトリックがあります。中央銀行もまた政府の法律に従っており、政府の利益のために動いています。つまり、操り人形使いが別の操り人形使いに操られているようなものです。表面上は中央銀行が主導しているように見えても、実際は政府の「必要な時に紙幣を刷る」という望みを間接的に果たしているのです。

これらのプレイヤーはさまざまな方法で利益を得ており、結果として複雑な支配構造が生まれています。政府は短期的な代償なしに資金を得られ、富裕層や銀行は簡単に利益を得ることができます。中央銀行はショーを続けさせます。

一方で、一般の人々はシステムが展開するにつれて影響を受け、課題に直面するかもしれません。

結局のところ、法定通貨システムの操り人形師たちは、ごく一部の者が大きな利益を得る一方で、多くの人々が「金融の舞台の公平さ」に疑問を抱くような茶番を作り出しているのです。



第4章



中央銀行の役割

中央銀行は経済の仕組みをそっと形作っています。彼らの公式な役割は安定性・信頼性を保ち、「物事を安定させる」ことですが、その手法には謎めいた側面もあります。

中央銀行は政府と密接に連携し、金利のような手段で通貨供給量をコントロールすることで、金融政策を操っています。

危機の際は何もないところからお金を印刷し、市中銀行を通じて経済に注入することで、あたかもすべてが順調かのように見せるのです。

中央銀行は単に監視しているだけではありません。市中銀行を規制し、ゲームのルールを定め、銀行が困ったときには「最後の貸し手」として介入・支援します。この支配構造の網は保護的に見えますが、経済や銀行を中央銀行にますます依存させています。

数兆ドル（日本円で数百兆円）規模の景気刺激策の資金がどこから来て、誰がどう配分を決めるのかを理解することは、より広い金融システムを理解する上で非常に重要です。

政府は、ある特定の時期に通貨供給量を管理するために、いくつかの手段を用いています。

中央銀行と政府は、金融政策や財政政策などの手段を通じて、通貨供給量や経済に影響を与えることができます。

例えば、アメリカの連邦準備制度（FRB）は金融政策によって金利を調整し、流通する貨幣量に影響を与えます。一方、財政政策は政府の支出や課税政策によって、経済活動に影響を与える手段です。

ターゲット指標

金融政策

失業率

6.5%未満

2% - 3%



国内総生産の年間成長率



コインフレ率
2.0% - 2.5%

拡張的財政政策

消費者支出と企業投資を増加させ、総需要と経済成長の拡大を目指す。



VS

緊縮的財政政策

消費者支出と企業投資を抑制し、過熱した経済成長を減速させたり、高インフレを防止・抑制したりすることを目指す



法定通貨とは何か？誰が管理している？

為替レート政策・供給ショック・価格統制なども、通貨供給量を調整し、貿易や経済に影響を与えるための追加的な手段として機能します。

これらの政策は物価の安定やインフレの抑制を目的としていますが、その介入はしばしば景気の過熱と低迷を繰り返すサイクルを引き起こし、管理された通貨を使うすべての人々に困難をもたらします。

例：「大きすぎて潰せない（Too big to fail）」

これは、その破綻が金融システム全体に壊滅的な影響を及ぼすほど、巨大かつ相互に結びついた金融機関を指します。

2008年の金融危機では、いくつかの大手銀行が「大きすぎて潰せない」と見なされ、アメリカ政府が介入して救済措置を講じ、その破綻を防ぎました。

金融危機における「大きすぎて潰せない」機関の有名な例の1つが、投資銀行のリーマン・ブラザーズでした。リーマン・ブラザーズが2008年9月に破綻申請をしたことで、保険大手のAIGが破綻寸前に陥ったり、

株価が大暴落したりするなど、ドミノ倒しのような連鎖的な影響が引き起こされました。

アメリカ政府はさらなる混乱を防ぎ、広範な経済を守るために、他の主要な金融機関に介入して救済措置を提供せざるを得ませんでした。

これらの政策がどのように機能するのかを知ることは、中央集権型の法定通貨システムの限界を理解する上で極めて重要です。問題を理解しなければ、解決策も見えてきません。

ここまで、法定通貨システムが過去と現在においてどのように機能してきたかを学んできました。最後に、法定通貨の未来である「中央銀行デジタル通貨（CBDC）」について見ていきましょう。

4.3 中央銀行デジタル通貨（CBDC）：法定通貨の未来

中央銀行デジタル通貨（CBDC）は、法定通貨の次なる段階です。紙幣や硬貨、デジタル決済の組み合わせではなく、政府が発行し中央銀行が管理する、完全にデジタルな形式の法定通貨です。

普段使っているお金を想像してください。

ただし、物理的な形は一切ありません。ポケットでジャラジャラと音を立てる小銭も、折りたたむ紙幣もありません。

CBDCの大きな特徴は、政府や中央銀行がかつてないレベルで管理・監視できるという点です。

CBDCによって、当局は金融取引を詳細に追跡し、資金の流れをより簡単に追跡・規制できるようになります。

政府と中央銀行は、CBDCの形式や供給量をすぐに調整でき、金利の操作や、金融・財政政策の手段をこれまで以上に高い精度で実行できます。

つまり、CBDCは当局にとって、より効率的に法定通貨を管理・運用するためのツールとなるのです。

CBDCは法定通貨の未来であるように見えますが、現在の世界の通貨システムはすでに純粋な法定通貨基準で動いています。

法定通貨はもはや金に裏付けられておらず、その結果、何の実際の制約もなく通貨供給量が大幅に増加しています。

法定通貨システムの仕組みがより明確になったところで、次の第5章では、その結果を探っていきましょう。

第5章： 問題は 解決策を生む

5.0 問題の紹介

5.1 購買力の低下

5.1.1 通貨インフレと購買力への影響

アクティビティ：インフレの影響 — オークション活動

5.2 世界的な債務負担と社会的不平等

5.2.1 個人への影響 — 購買力の喪失

5.2.2 社会への影響 — 富の格差の拡大

アクティビティ：法定通貨システムの結末

5.2.3 世界的な債務負担

5.3 サイファーパンクと分散型通貨の探求

5.3.1 サイファーパンク

5.3.2 中央集権型システムと分散型システム

5.3.3 デジタル通貨の簡単な歴史

生徒用ワークブック

日本語版 | 2025年版

問題は解決策を生む

5.0 問題の紹介

我が国における通貨の流通量を支配する者は、すべての産業と商業の絶対的な支配者である。この仕組み全体が、多かれ少なかれ、頂点にいる少数の権力者によって極めて容易に支配されていることに気づけば、インフレや恐慌の時代がどのように発生するのかを説明される必要はないだろう。

ジェームズ・A・ガーフィールド（アメリカ合衆国大統領）

第4章では、金融の世界は見た目ほどには強いとは言えない仕組みに依存していることを学びました。法定通貨システムは、紙幣の継続的な供給によって支えられており、恩恵を受けるのは多くの人ではなくごく一部の人々のようです。

本章では、法定通貨システムが一般の人々や社会にとって何を意味するのかを明らかにします。そして最後に、これらの問題に気づき、人類社会の未来を変える可能性のある解決策を見つけるために、静かに探求した人々の物語に触れます。

5.1 購買力の低下

5.1.1 通貨インフレと購買力への影響

通貨インフレとは、経済全体における通貨供給量の増加を指し、一般の人々にとっては購買力の低下という形で直接的な影響をもたらします。

物価インフレのサイクルは、市場に出回るお金が増えることで始まります。結果として、モノやサービスへの需要を高め、最終的には物価の上昇を引き起こします。

アレックス、ボブ、チャーリーという友人3人組を想像してみましょう。それぞれが100円を持っていて、売り物の水が1本あります。最初の状況はシンプルで、3人が合計300円、そして水は1本です。ここで、例えば地方政府が3人それぞれにもう100円ずつ配布すると、彼らは合計で600円を持つことになります。新たなお金を手にしたことで、彼らはその1本の水を買いたくなります。みんなが同じ1本の水を欲しがるため、競り合いの開始です。

追加で与えられたお金によって需要が高まり、3人は水のボトルに対して当初よりも高い価格を提示するようになります。結果として、競り合いによって水の価格は上昇しました。

この状況は、3人の購買力が低下したことを表しています。お金は増えたはずなのに、以前のようにたくさんの水のボトルを買うことはできません。これは、彼らのお金の価値に対するインフレの影響を示しています。

この例では、友たちは政府によって配布された円のような、外的要因の影響を受ける通貨を使っていたため、購買力の低下を経験しました。通貨供給量に対するコントロールが効かず、需要の増加と相まって物価が上昇し、追加で与えられた円を持っていても以前と同じ量のモノを買うのが難しくなったのです。

これは、購買力が自分たちの手の届かない要因によって左右されることを示しており、私たちのお金の価値に影響を与える仕組みを理解し、疑問を持つことの重要性を浮き彫りにしています。

では、これらの影響が実生活でどのように現れるのかを見ていきましょう。

第5章

アクティビティ：インフレの影響 —オークション活動

目的：

経済において、インフレがモノやサービスの価格にどのように影響するかを理解する。

定義：

 通貨供給量（マネーサプライ）：特定の時点で経済全体に流通しているお金の総量。

含まれるもの：

- 硬貨や紙幣などの物理的な通貨
- 当座預金
- 普通預金
- マネーマーケット口座
- 小口定期預金（譲渡性預金証書など）

 オークション：モノや財産が、最も高い金額を提示した人に売却される公開形式の販売方法。

クラス演習 — 以下の手順に従ってください：

- 1.先生からランダムな金額のゲーム用紙幣が配られます。これは社会における通貨供給量を表しています。
- 2.配布された紙幣の合計金額を、配布された表に記録してください。
- 3.先生がキャンディバーをオークション形式で販売します。キャンディバーを手に入れるには、ゲーム紙幣で最高額の入札をする必要があります。勝者の落札額を通貨供給量の隣に記録しましょう。
- 4.先生が通貨供給量に大きな金額を追加します。これは経済における通貨供給量の増加を表しています。
後ほど、経済における通貨供給量がどのように増減するかを学びます。



社会はしばしば予測不可能で不公平なものであり、先生が一部の生徒にだけ多額のお金をランダムに与えるというシミュレーションはその一例です。これは、現実世界における資源や機会の不平等な分配を再現しており、社会に存在するランダム性や不公平さを浮き彫りにしています。

- 5.先生は、同じ手順で2つ目のキャンディバーをオークションにかけます。勝者の落札額を通貨供給量の隣に記録しましょう。
- 6.先生はさらに3回目のオークションを実施します。

問題は解決策を生む

ラウンド	通貨供給量	落札額
1		
2		
3		

まとめ：

1. 通貨供給量の増加は、キャンディバーの落札額にどのような影響を与えたか？
2. 通貨供給量の増加とインフレにはどのような関係がありますか？
3. 現実の社会において、通貨供給量はどのように関係しているのでしょうか？
4. 経済に新たなお金が投入された場合、モノやサービスの価格はどうなると思いますか？価格の変化は一時的だと思いますか、それとも永続的だと思いますか、またその理由は何ですか？価格変動は長期的に市民にどのような影響を与えると思いますか？

5.2 世界的な債務負担と社会的不平等

5.2.1 個人への影響 — 購買力の喪失

ハイメは小さなアパートに住む大学生です。生活費と学費を稼ぐために、カフェでアルバイトをしています。一人暮らしを始めてすぐに、ハイメは自分で家計簿をつけるのが得意になりました。



家計簿とは、自分のお金のやり取りをすべて記録する詳細な帳簿のことです。収入でも支出でも、家計簿をつけることで、お金の流れを追跡するのに役立ちます。

2023年の初め、彼は家賃・食費・その他の生活必需品を含む1年分の生活費として、100万円の予算を立てました。

以下は、2023年1月に行ったお金のやり取りの記録です。

第5章

日付	内容	金額	種類	残高
2023/01/01	開始時残高			16万円
2023/01/01	1月分の家賃	8万円	支出（借方）	8万円
2023/01/05	食料品	1万円	支出（借方）	7万円
2023/01/15	アルバイトの給料	5万円	収入（貸方）	12万円
2023/01/20	車のガソリン代	3万5000円	支出（借方）	8万5000円
2023/01/30	教科書	1万5000円	支出（借方）	7万円

この家計簿からわかるように、ハイメの初期残高は16万円で、そのうち8万円を家賃の支払いに使いました（支出）。次に1万円を食料品に使い、アルバイトの給料として5万円（収入）を受け取り、残高は12万円になりました。その後、ガソリン代と教科書代を支出し、月末には残高が7万円になりました。

12か月後、ハイメは祖父と昼食をとりながら、2024年の予算について話しています。

ハイメは、以前よりも予算が持たなくなっていることや、過去1年間で生活費が大幅に増加していることに気づきます。その理由を考えていると、祖父が1枚の画像を見せてくれました。

ハイメは目を疑いました。

モノやサービスの価格は時間の経過とともに大きく上昇し、それによって自分の購買力が下がっていたことに、彼は初めて気づいたのです。

祖父は言います。

「1956年、私は社会に出たばかりの若者だった。工場で働いて月収は3万8000円だったよ。」

今では大した額に思えないかもしれないが、当時としては十分な給料だった。実際、そのお金を少しずつ貯めて、郊外に自分の家を買うことができたからね。」

「昔と今では、物の値段は全然違うんだ。

例えば2020年にハーシーのチョコレートバーを30本買おうとしたら、2614円かかった。

でも1913年に戻れば、同じ30本がたったの100円だったんだよ。」

このような大きな価格差は、時間の経過による購買力の変化や、インフレによってどのように変化してきたかを浮き彫りにしています。



注釈：金額のイメージをつかみやすくするため、原文のドル表記を1ドル=100円として換算し、記載しています。（実際の為替レートとは異なります）

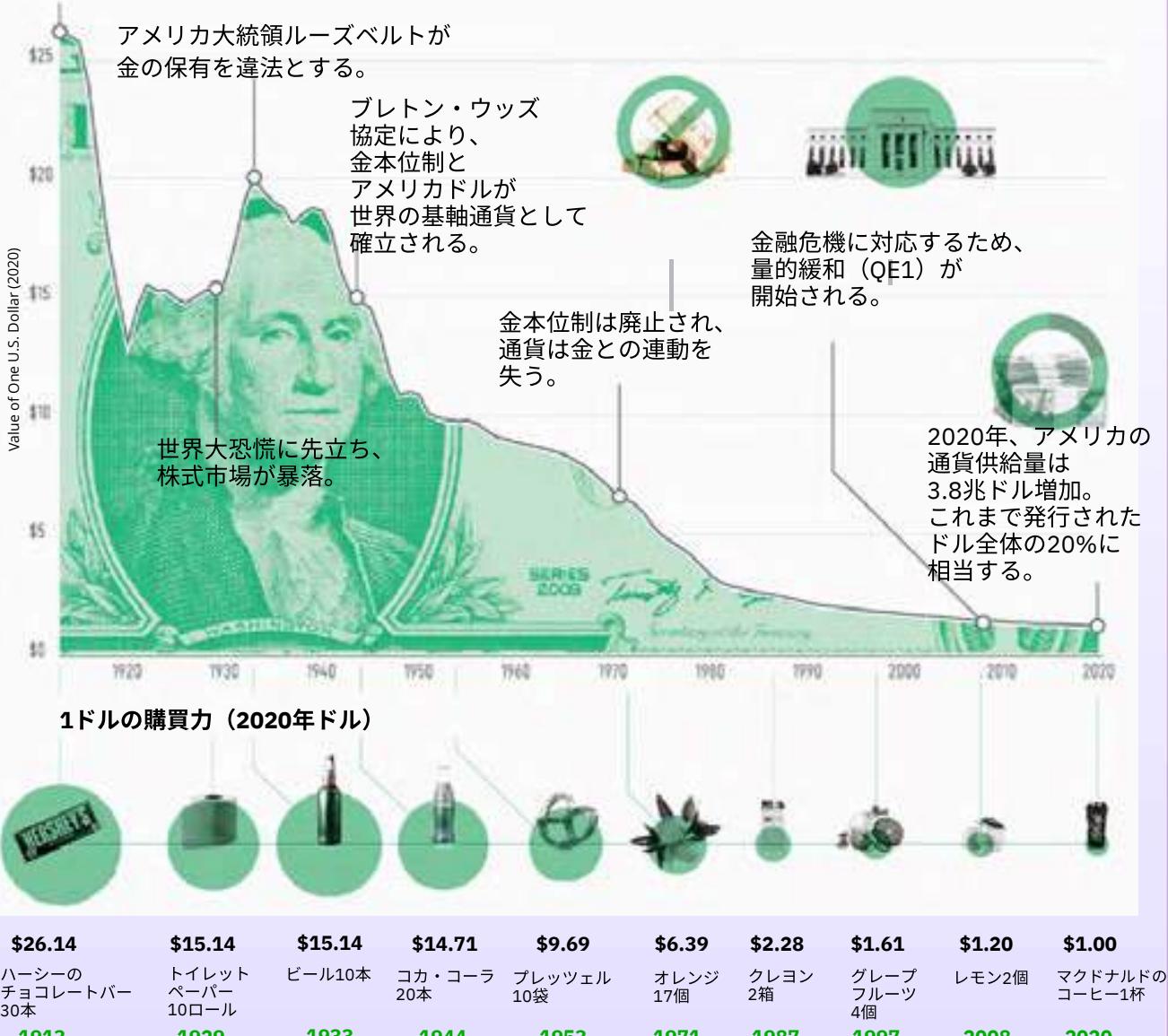
問題は解決策を生む

1ドルの価値

アメリカドルの購買力

連邦準備法により、国の通貨供給量を管理する能力を持つ中央銀行が設立される。

- インフレと通貨供給量の増加により、過去100年でアメリカドルの購買力は大幅に低下。



ハイメ：「えっ？信じられない！昔の家賃って、今と比べてどれだけ安かったんだろう…想像もつかないよ。」

祖父：「そうだね、その頃なら家賃はずっと安かったよ。

もう1つ例を挙げると、昔なら100円あればプレッツェルが10袋くらい買えたんだ。

でも2020年には、同じ量に969円も払ったよ。

今ならいくらかかるか想像してごらん。」

第5章

ハイメ：「わあ、おじいちゃん、本当に面白いね。おじいちゃんは若い頃に、実際にその状況をどう体験したの？」
 祖父：「ああ、ハイメ、昔は何もかもが本当に安かったんだよ。パン1斤が18円で、ガソリン1ガロン（約2.8キロ）もたったの29円だったんだ。今の生活費の高さは信じられないよ。」

祖父との会話の後、ハイメは家に戻って、自分の家計簿をもう一度見直しています。
 すると、前年と同じ量のモノやサービスを購入するためには、2024年の予算をさらに10万円上乗せしなければならないことにすぐ気づきました。
 これはつまり、同じものを買うのにより多くのお金が必要になったため、ハイメの購買力が10万円分下がったことを意味します。
 一方で、ハイメの給料はわずかしか増えておらず、生活費だけが毎年急激に上がっているのです。

以下の表は、ハイメの1年目と2年目の費用、そして価格上昇率を示しています。
 ハイメが同じ生活水準を維持するためには、週あたりの労働時間を増やして、追加の10万円を稼ぐ必要があります。
 アメリカ労働統計局の情報によると、現在の物価は1913年と比べて約30倍に上昇しました。
 これは、現在の1ドルが、当時買ったものの約3%しか買えないことを意味します。

項目	1年目の費用	2年目の費用	増加率
家賃	\$4,000	\$4,500	12.5%
食料品	\$2,000	\$2,300	15%
生活必需品	\$4,000	\$4,500	5%
合計	\$10,000	\$11,000	10%

例えば、「1913年に100ドルをもらうか、2023年まで待って3ドルを受け取るか」というタイムトラベルの選択をハイメに提示いたします。

これは、過去にたっぷり買い物ができたのに対し、今ではほんの少しのおやつしか買えないようなものです。

これほどの価値の差は、お金の購買力が年月を経てどれほど低下したかを示しています。

1938年の生活費

生活費

- ・新築住宅：3,900ドル
- ・平均年収：1,731ドル
- ・新車：860ドル
- ・平均家賃：月27ドル
- ・ハーバード大学の授業料：年420ドル
- ・映画チケット：1枚25セント
- ・ガソリン：1ガロン10セント
- ・アメリカの郵便切手：1枚3セント

食品

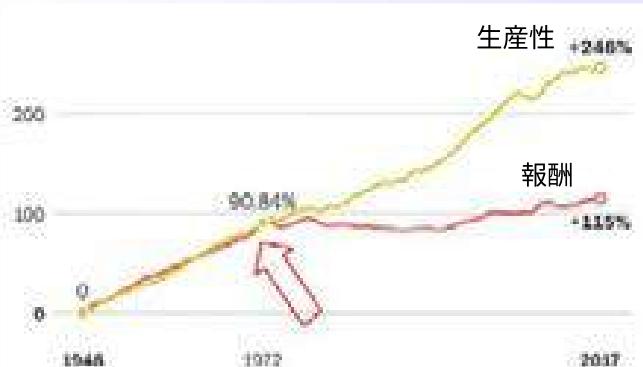
- ・グラニュー糖：10ポンドで59セント
- ・ビタミンD入りミルク：1ガロン50セント
- ・ベーコン：1ポンド39セント
- ・コーヒー豆：1ポンド32セント
- ・卵：1ダース18セント

(Based on the original image)

問題は解決策を生む

数字だけを見ると、ハイメが1年間に稼ぐお金は祖父が稼いだ額より多いのですが、祖父が持っていたお金の方がはあるかに価値があり、当時はもっと多くのものが買えたのです。

生産性と時給報酬の伸び（1948年～2017年）



注：報酬には、生産部門および非管理職の労働者に対する賃金と福利厚生が含まれます。

今日の世界では、インフレの大きな影響が人々の貯蓄意欲を削いでいます。

多くの人はすぐにお金を使う道を選びます。なぜなら、お金の価値が急速に下がってしまうからです。このような悲観的な見通しは、彼らが将来の計画を立てる能力を妨げます。

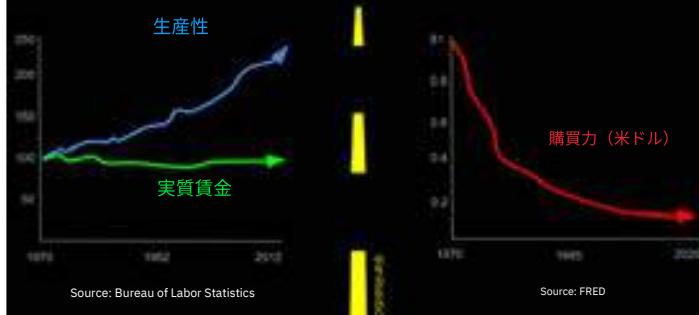
グラフからも分かるように、平均的な人の給与の伸びはインフレ調整後ではほとんど停滞しており、懸命に働いても、お金の価値の下落スピードに見合った賃上げを受けられていません。

ハイメの例は、ほんの一例にすぎません。法定通貨の世界では、政府が自らの目的を達成するために、何もないところからお金を生み出すことはごく一般的です。

そしてその影響を受けるのは、世界中の一般市民です。パンから住宅、食料品から休暇に至るまで、あらゆる生活必需品の価格が毎年上がっていきます。

資産を持つ裕福な人々はインフレの恩恵を受けますが、一般の人々は苦労して稼いだお金の価値が失われるのを見ているしかありません。その結果、世界中の人々や家族が購買力の低下に苦しんでいるのです。

The Road to Serfdom (隸属への道)



世界中の人々が、同じ生活水準を維持するために、複数の仕事を掛け持ちし、より長時間働くことを強いられています。まるでルームランナーの上を走っているようなもので、どれだけ速く走っても前に進めないです。

法定通貨システムの中で、個人は物価上昇との終わりのない競争にさらされているように感じます。

第5章

生活費の上昇に対応するため、多くの人々は「クレジット（借金）」に頼るようになります。これは、まるで深い傷に小さな絆創膏を貼るようなものです。人々はなんとかその日をしのぐためにローンを組んだり、衝動的な意思決定をしたりします。目先の現金が必要不可欠となり、今日を生き延びることが明日への計画よりも優先されるサイクルに陥ってしまうのです。

法定通貨システムは、際限のない紙幣発行によって人間の心理に影響を与え、高い時間選好を植え付けます。つまり、長期的な計画よりも短期的な利益を優先する傾向です。即効性のある対処を求めるように、法定通貨の世界では短期的な利益を優先する人が多くなるのです。それは生存本能からくるものであり、長期的には持続不可能であっても、あらゆる手段を使って即座にお金を得ようとする依存のサイクルを生み出します。

本質的に、法定通貨システムの影響は、世界中の人々にとって厳しい現実を浮き彫りにしています。この仕組みの中では、物価は上がり、収入は停滞し、生き延びることそのものが日々の闘いになります。特定の集団が富を得る一方で、世界中の大多数の人々は、彼らをますます貧しくするシステムに依存せざるを得ないのでしょう。

5.2.2 社会への影響 – 富の格差の拡大

健全な通貨を基盤とした社会では、政府の財政上の決定は人々の承認にしばられています。しかし、法定通貨システムでは、政府は国民に負担を押し付けながら無制限に借金を重ねることができます。

紙幣を自由に印刷できる権限は、しばしば政治の中央集権化を引き起こします。法定通貨システムによって、政府は莫大な借金を抱えることができ、国民の大多数よりも自分の利益になるような判断を下せるようになるのです。

アメリカのような超大国は、この仕組みによって競争上の優位を得ています。彼らは際限なく紙幣を印刷して、戦争を含む自国の計画に資金を投入できます。この能力によって、こうした支配的な国家は地政学的な紛争を支配し、影響を及ぼし、関与することが可能となり、世界的な力の不均衡を生み出しているのです。超大国にとっては、他国を支配するための戦争や大規模な行動が財政的に可能になる一方で、財政的な柔軟性を持たない国々は制限に直面します。

法定通貨システムのもとでは、富は平等に分配されません。むしろ、ごく一部の人々の手に集中していく傾向があります。この現象は、モノポリーというボードゲームで、少数のプレイヤーがほとんどすべてのホテルや土地を所有し、大多数のプレイヤーが破産寸前でもがいているような状況に似ています。

法定通貨システムは、特定の集団が富を集中させるための道具となっています。政府と中央銀行が連携して紙幣を刷ることで経済に通貨を流し込みますが、その恩恵を最初に受け取るのは、すでに富と地位を持っている人々——つまり権力を持った組織や個人です。

こうした人々は、購買力の低下といった悪影響が経済全体に現れ始める前に、刷りたてのお金から利益を得るのです。

問題は解決策を生む

富の不平等は、単に持つ者と持たざる者の違いにとどまりません。それは経済的な流動性を抑圧するものなのです。恵まれない境遇の人々は、経済的な階段を昇ることはますます困難になっており、まるで重いリュックを背負って競争を始めるようなものです。

富裕層と貧困層の格差が広がると、すべての人にとって問題が生じます。富裕層は自分たちに有利な政策を作り、それが一般の人々をさらに苦しめます。その結果、社会的不安や制度への不信感、そして地域社会が砂上の楼閣のように崩れ落ちる状況を引き起こすのです。

法定通貨システムの不安定さは、経済的な不確実性や政治的不安、そして欧米諸国が景気後退に直面した際に世界的な影響として現れます。

これは、先進国と発展途上国の両方に影響を与えるグローバルな現象です。時には裕福な個人や集団がこの機会を利用して、世界の金融システムを自らの利益のために利用し、上層階級と下層階級の格差をさらに広げることもあります。

法定通貨システムのもとでは、借金をすることが人類にとって当たり前になりました。政府・機関・企業、そして世界中の個人が、借金の海に浸かっているのです。

借金が容認されるという心理的な変化の根源には、法定通貨システムの設計があります。過去数十年間にわたって、あらゆる組織が多額の借金をしやすくなり、物価と生活費の上昇により、一般の人々にとっても借金が必要不可欠になってきました。

消費主義、つまり常に買い求め続ける衝動は、人々に必要以上の買い物をさせ、過剰消費や無駄を生み出します。終わりのないショッピングの連鎖のように思えるかもしれません、本当の代償は値札以上のものであり、人々の心理的な健康や幸福にまで悪影響を及ぼします。

法定通貨システムが単なる経済メカニズムではないことは明らかです。むしろ、それは人間社会全体のあり方を形作るシステムなのです。権力の集中からグローバルな動向・富の格差・社会的な規範に至るまで、法定通貨システムは国家の運営や一般市民の生き方に直接的な影響を及ぼします。

アクティビティ：法定通貨システムの結果

1. 法定通貨システムの結果として、個人や社会全体が経験している他の影響はありますか？
2. あなたの国では、法定通貨システムによりどのような影響がありましたか？歴史を振り返ったとき、何が起こり、人々にどのような影響を与えたか？

a. 個人的な体験談をクラスやグループで共有しましょう。



第5章

5.2.3 世界的な債務負担

法定通貨システムの結果として、世界中の政府は「グローバルな債務スパイラル」と呼ばれる、巨大な借金の網に絡め取られています。

あなたが決して返済しきれないほどの借金を抱えている状況を想像してみてください。今、まさにそれが世界規模で起きているのです。

政府は借金まみれとなり、返済不可能なレベルで負債を積み重ねる危険なゲームに巻き込まれています。

これは、無謀な支出と借り入れ、そして将来を見据える力の欠如が生み出した物語であり、世界中の国々を財政破綻の瀬戸際に追い込んでいます。



アメリカ連邦政府は2019年以降、なんと1兆ドルもの新たな借金を積み重ねてきました。

総債務は2019年第4四半期の約23兆ドルから、現在では34兆ドルという驚異的な額にまで膨れ上がっています。

世界中の政府が新たな借金を生み出すスピードは衰えるどころか、むしろ加速しています。

2023年は、新型コロナウイルス感染症のパンデミックに見舞われた2021年以来、最も債務が増加する年になると予測されていました。

世界の政府債務の状況



では、すでに法定通貨システムの影響に苦しんでいる個人や社会にとって、これは何を意味するのでしょうか？

彼らが巻き込まれている債務スパイラルは、坂を転がり落ちる雪玉のようにどんどん大きくなっていき、もはや止め方すら分からない状態です。

先に述べた、富の不平等や社会の不安といった影響が消えることはありません。それどころか、世界的な債務負担はもはや引き返せない地点に達しており、事態がさらに悪化する運命にあることを示しています。

対GDP比 2021年 (%)

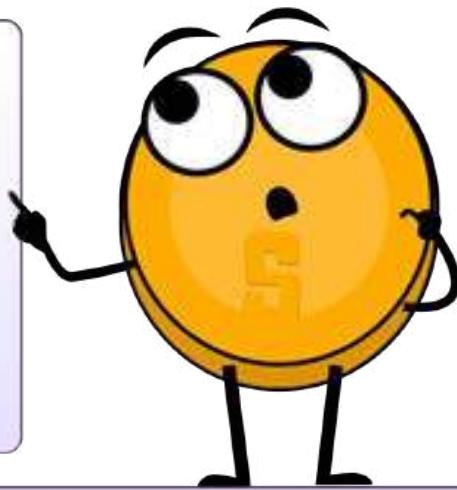


問題は解決策を生む

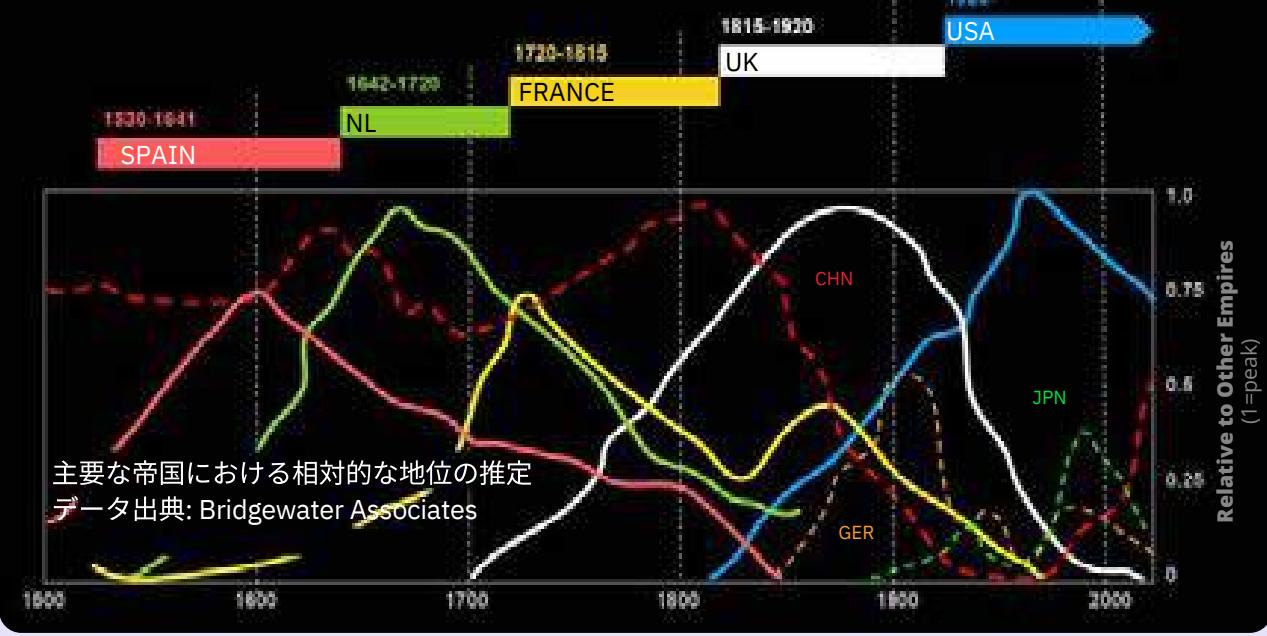


“健全な貨幣を再び手にすることは、政府の手からその支配権を取り上げるまでは決して実現しないと私は信じている。
私たちにできるのは、
政府が止められないような何かを、
巧妙に、遠回しな方法で導入することだけだ。”

フリードリヒ・ハイエク
ノーベル経済学賞受賞者



世界の基軸通貨



5.3 サイファーパンクと分散型通貨の探求

歴史を通じて、銀行と政府が貨幣を徐々に支配してきた過程を私たちは見てきました。
結果として生まれたのは、今日私たちが知る法定通貨システムであり、それが社会にもたらす悲惨な結果につながっています。

しかし、暗号技術やインターネットといった新しいテクノロジーの登場により、政府の介入を受けず、誰もが自由にアクセスできる、独立したデジタル通貨という新たなアイデアが生まれました。
この革命的な運動を主導する人々、すなわちサイファーパンクの旅をたどってみましょう。

第5章

5.3.1 サイファーパンク

コンピューターは、人々を支配するためではなく、解放し守るための道具として使われるべきだ。

ハル・フィニー

20世紀後半には、コンピューターやインターネットといった複数の革新的技術が登場し、新たなデジタル時代への道が開かれました。

あるグループの人々は、これらの技術が社会の仕組みを大きく変えると気づきます。彼らはパソコンの可能性と危険性の両方を予見しており、個人に自由をもたらす道具になるか、あるいは監視と支配のための手段になるかという岐路にあることを理解していました。

こうした考えを持つ人々は「サイファーパンク」と呼ばれました。彼らは、プライバシー・セキュリティ・分散型のデジタルな未来という共通のビジョンを共有する、ゆるやかに結びついた活動家・暗号学者・プログラマー・プライバシー活動家のグループとして出現しました。「サイファーパンク」という言葉は、「暗号（cypher）」と、反主流の精神を表す「パンク（punk）」を組み合わせた造語です。

彼らは、暗号技術には個人の自由を守る力があると信じていました。オンライン通信の安全確保、インターネット上の匿名性の向上、そして中央集権の支配を受けないデジタル通貨の確立が彼らの目標の1つでした。

サイファーパンクは、法定通貨システムの問題点を理解し、「オーウェル的未来」の脅威を認識していました。彼らは、パソコンやインターネットが国家による国民支配を強める道具ではなく、人類にとって有益なものとなるようにしなければならないと信じていました。

オーウェル的未来の定義：



オーウェル的未来とは、ジョージ・オーウェルの著作に着想を得た、ディストピア（ユートピアの反対）的な未来像を指します。

この用語は、抑圧的な政府の支配・大規模な監視・プロパガンダ・情報操作などを特徴とする、悪夢のような全体主義社会と関連付けられています。

「オーウェル的」という言葉はしばしば、国民の自由や個人の自律性が厳しく制限され、反対意見が抑え込まれ、現実が権力者の都合で歪められるような状況を表すために使われます。

この概念は、ジョージ・オルウェルにちなんで名付けられました。彼はその著作の中で、抑制されない国家権力と基本的人権の侵害がもたらす潜在的な危険性について警鐘を鳴らしています。

問題は解決策を生む

サイファーパンク運動の中心人物には、エリック・ヒューズ、ティモシー・C・メイ、ジョン・ギルモアといった著名な人物が含まれていました。

1992年、エリック・ヒューズは「サイファーパンク宣言（マニフェスト）」を執筆し、グループの原則を明確に示しました。この宣言では、プライバシー、暗号技術、そして個人が自分自身のデジタルアイデンティティを管理する重要性が強調されています。

サイファーパンクの最も注目すべき発明の1つが、暗号ツールとプロトコルの開発でした。1991年、フィル・ジマーマンは「PGP（Pretty Good Privacy）」という電子メール暗号化ソフトウェアを発表し、これが代表的なプロジェクトとなりました。PGPによって、ユーザーはインターネット上で暗号化されたメッセージを送信できるようになりました。受信者以外には内容を解読できなくなっています。それ以前は、インターネットで送信されたメッセージは政府などによって傍受・閲覧される可能性がありました。

サイファーパンクは、暗号技術の進歩に加えて、インターネットやコンピューターの登場によって、デジタル空間における分散型ネットワークの構築に適した土台が整ったと考えていました。個人が中央集権的な干渉を受けずに、インターネット上でプライバシーを保った通信や取引ができるようになると考えたのです。

サイファーパンクは、テクノロジーが支配の道具ではなく、自由を最大限に引き出すための道具となるような、人類にとってより明るい未来を築く道を歩んでいました。欠けていたのは、分散型ネットワークとデジタル通貨だけでした。

5.3.2 中央集権型システムと分散型システム

中央集権型システム：1人の支配者、多くの問題

中央集権型システムでは、すべてが1つの中心的な権力のもとで動きます。都市の中の高層ビルのように、その権力がシステム全体の働きをコントロールしているのです。

伝統的な銀行を例に挙げると、少人数の集団がすべての意思決定を行っています。

- 現実の例：2022年、カナダで平和的な抗議活動が行われた際、銀行が抗議者たちの口座を凍結しました。これは、中央権力が介入し、金融へのアクセスを制限できることを示しています。



この動画を見て、
サイファーパンクの
物語を知ろう！



第5章

中央集権型システムの問題点：

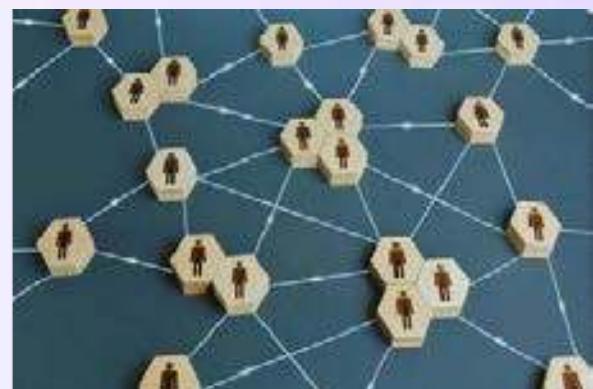
- ◆ 単一障害点：中央の権限に問題が生じると、システム全体が崩壊するおそれがある。
- ◆ コントロール：ごく一部の上層部がすべての制御権と権力を持ち、しばしば自分たちに有利な判断を下すことがある。
- ◆ 非効率性と仲介者の存在：都市の渋滞のように、不要な仲介者のせいで中央集権型システムは遅くなり、コストがかさむことがある。
- ◆ 自律性の欠如：個人が自分の金融選択をできず、すべて上位の権力者によって決められることがある。
- ◆ 検閲と制限：都市の一部が封鎖されることがあるように、中央集権型のシステムは特定の金融資源へのアクセスをブロックまたは制限することがある。
- ◆ 拡張性の課題：金融サービスを必要とする人が増えると、中央集権型のシステムでは対応が難しくなることがある。
- ◆ セキュリティリスク：中央の権限に問題があると、システム全体がサイバー攻撃のリスクにさらされる可能性がある。
- ◆ 透明性と信頼の欠如：中央集権型のシステムの内部構造は分かりにくく、人々がそれを信頼するのは難しい場合がある。

分散型システム：人々に力を

今度は、分散型のシステムを大きな森だと考えてみてください。

それぞれの木が独立した部分を表し、森全体がシステム全体を表します。1つの中心点がある都市とは違い、分散型システムはどこか一部に問題があっても全体が機能し続けられる、強靭な森のようなものです。

- ◆ 現実世界の例：Torネットワークとそのブラウザは、人々がインターネット上で匿名性を保てるようにし、ネットワークを停止したり検閲したりすることが困難な分散型システムを構築しています。



分散型システムの利点：

- ◆ 強化された回復力と信頼性：単一障害点がないため、何らかの問題が発生してもシステム全体が強固に保たれます。
- ◆ セキュリティの向上：適切な暗号化や保護措置を講じれば、分散型システムは中央からの支配に対してより抵抗力があります。

問題は解決策を生む

- ◆ より大きな主権の獲得：人々は自分のお金、データ、意思決定をよりコントロールできるようになる。
- ◆ 透明性の向上：誰もが同じ情報を確認できるため、システムに対する信頼が高まる。
- ◆ 許可不要かつ無制限な性質：誰でも参加できるため、包摂的な金融システムになる。
- ◆ 平等な機会：誰もが公平に参加し、発言する機会を持つ。
- ◆ プライバシーの向上：データは複数の参加者に分散され、主に匿名化されているため、分散型システムはよりプライバシーが保護される。

分散型システムには多くの利点がありますが、みんなで意思決定を行うのは少し難しいこともあります。全員の協力が必要です。

権力の行使方法を変える

中央集権型システムと分散型のシステムの世界では、「誰が権力を持っているか」が重要です。

中央集権型のシステムでは少数の集団に権力が集中しますが、分散型のシステムではそれを分散させ、誰もが発言権を持つようになります。

このような権力の移行は、多くの人々が自分たちの生活を形作るシステムに影響を与えられる、より公平で民主的な未来を意味します。

5.3.3 デジタル通貨の簡単な歴史

サイファーパンクが議論した最も重要な概念の1つがデジタルキャッシュです。

彼らは、「国家」と「お金」を切り離すことで、より多くの人々のためになる未来が訪れると考えました。

デヴィッド・チャウムによる、暗号プロトコルに関する先駆的な研究は、安全でプライバシー保護された取引の基盤を築きました。

ただし、このプロトコルは効率的に機能させるために中央の権限が必要だったため、単一障害点や検閲の可能性に対する懸念が生じました。

その後の数年間、複数のサイファーパンクが互いのアイデアを改良し、政府の管理を受けない実用的なデジタル通貨の実現を目指して挑戦を続けました。

以下の表は、彼らがデジタルキャッシュの実現に向けて開発した主要なイノベーションを紹介したものです。

名称と日付	説明	限界
E-Cash (1982)	デヴィッド・チャウムによる、初期の電子キャッシュの概念。暗号技術によるプライバシー保護を重視した。	中央の権限が必要であり、単一障害点や検閲の懸念があった。
DigiCash (1990)	デヴィッド・チャウムが設立した企業。プライバシーを重視したデジタル通貨の実現を目指した。	中央集権型モデルが影響し、最終的に1998年に破綻した。

第5章

B-money (1996)	ウェイ・ダイによって提唱された、匿名かつ分散型の電子キャッシュシステムに関する理論的な提案。	実践的な実装を欠き、概念的なアイデアにとどまった。
Hashcash (1998)	アダム・バッカが開発した、スパムメールやサービス妨害攻撃（DoS）を制限するために設計されたブルーフ・オブ・ワーク方式のシステム。	デジタル通貨における二重支払いの問題には直接対応していなかった。
Bit Gold (1998)	ニック・サボが提案した、ブルーフ・オブ・ワークの要素を含む分散型デジタル通貨システムの構想。	実装されず、理論上の概念にとどまった。
e-Gold (2004)	物理的な金を裏付けとした中央集権型デジタル通貨。 ユーザーはe-Gold単位を購入・送金できた。	法的問題により2009年に閉鎖され、中央集権型デジタル通貨の課題が浮き彫りになった。

サイファーパンクは特定の組織や政府に支配されないデジタル通貨を作ろうと、何十年にもわたって数多くの試みを重ねてきましたが、その努力は実践的な課題に直面し、現実の世界で完全に実現することはありませんでした。安全性、拡張性、そして広く普及する可能性のあるデジタルキャッシュを構築するのは容易ではないと、彼らは結論づけました。

しかしこの物語は、ある人物が登場することで転機を迎えます。この人物は、サイファーパンクの教訓を学び、分散型デジタル通貨の概念を新たな高みへと押し上げたのです。

次の章では、40年にわたるこれまでの先行研究を基にしたこの人物の貢献が、最終的に機能するシステムを生み出すに至った経緯を探ります。

第6章： ビットコイン 入門

6.0 サトシ・ナカモトとビットコインの誕生

6.1 ビットコインはどのように機能するのか？

6.1.1 ナカモト・コンセンサス・メカニズム

6.1.2 ゲームプレイヤーたち

アクティビティ：ピア・ツー・ピア（P2P）ネットワークにおける合意形成

6.2 健全なデジタルマネーとしてのビットコイン

6.2.1 はじめに

6.2.2 ビットコインの特徴

アクティビティ：クラスディスカッション——ビットコインは「健全なお金」か？

6.2.3 自己責任を受け入れる

生徒用ワークブック

日本語版 | 2025年版

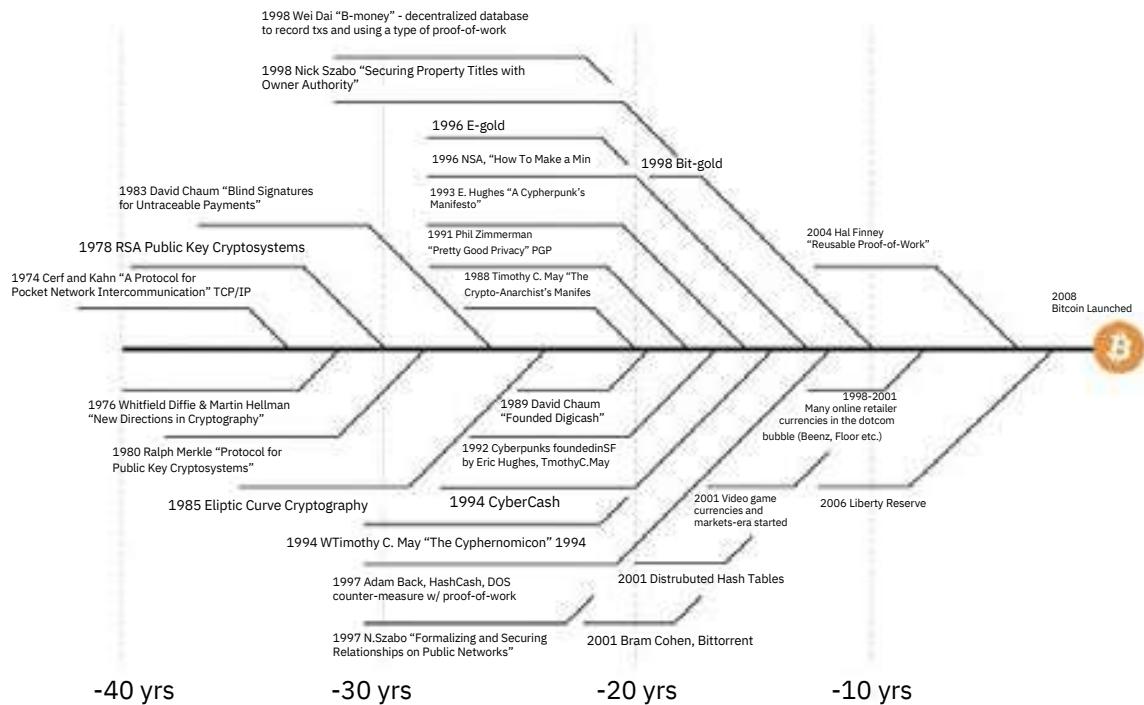
ビットコイン入門

第6章：ビットコイン入門

多くの人々は、1990年代以降に失敗した数々の企業を理由に、
電子通貨を最初から無理なものだと決めつけてしまう。
しかし、それらのシステムを失敗に導いたのは、
中央集権的な性質にほかならないことは明らかだ。
信頼に基づかない分散型のシステムを試すのは、今回が初めての機会だと私は思う。

サトシ・ナカモト

ビットコインの前史： それは、40年にわたる研究・開発・需要の賜物である



前の章で読んだように、複数のサイファーパンクが代替的な貨幣システムを作ろうと試みました。この章では、そのうちの1人、「サトシ・ナカモト」という名の先見の明を持った人物の物語を続けていきます。

この匿名の人物（男性、女性、あるいはグループ）は、ビットコイン登場以前から、暗号学を愛好するコンピューター科学者やハッカーたちと同様に、法定通貨システムに代わる実践的な解決策を模索する動きに関心を寄せていました。

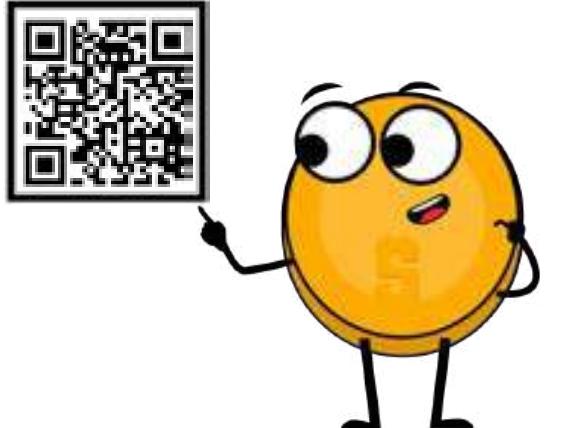
第6章



2008年10月、サトシ・ナカモトは暗号学関連のメーリングリスト上で、『Bitcoin: A Peer-to-Peer Electronic Cash System (ビットコイン：ピア・ツー・ピア電子通貨システム)』と題された画期的なホワイトペーパーを発表しました。

この文書は、仲介者を必要とせずに安全なオンライン取引を可能にする、分散型ピア・ツー・ピア（P2P）プロトコルの基礎を築いたものです。

サトシの構想は明確でした。強力な政府や金融機関の支配から解放された、純粋なピア・ツー・ピア型の電子キャッシュを創り出すことです。



そして2009年1月3日、サトシは
「ジェネシス・ブロック」と呼ばれる
最初のビットコインブロックを
採掘しました。

これはビットコインネットワークの
正式な始動を意味し、分散型台帳によって
信頼とセキュリティを基盤にした
新たな貨幣システムが誕生した瞬間です。

その後数か月、そして数年にわたり、次第に多くの熱心な支持者がこのアイデアに参加し、貢献するようになりました。

Bitcoin Genesis Block

RawHexVersion

2011年、ビットコインネットワークが影響力ある創設者なしでも正常に機能することを証明した後、サトシは別のビットコイン開発者にメールを送り、自分はビットコインの表舞台から身を引き、その未来同じビジョンを共有する他の「良き手」に委ねると伝えました。

サトシの正体はいまだ謎に包まれたままでですが、ビットコインを作った目的は決して謎ではありません。ビットコインは本質的に、少数の者に集中していた権力を奪い、多くの人々の手に取り戻すために、分散型・オープンソース・透明性のある新しい貨幣システムとして構想されたものであり、お金と国家の分離を目指したものでした。

ビットコインの創造は、2008年の金融危機に対するサトシの答えでもありました。この危機は世界中の一般市民を苦しめる一方で、再びエリート層を富ませたのです。

ビットコインは、腐敗と脆弱さを抱えた法定通貨システムに対するサトシの回答です。サトシは新たな革命の土台を築いたにもかかわらず、名声を求めることがなくその場を去りました。

ビットコイン入門

その後の数年間で、ビットコインは急速に成長し、希望・自立・回復力の象徴として台頭しました。

法定通貨システムに挑戦し、安全で検閲耐性がある金融取引手段を提供しています。

ビットコインはオープンソースプロトコルであり、誰かが所有・支配する権限はありません。

その設計は公開されており、誰でも参加できます。

現在、国境のない透明で安全な金融システムというビットコインの理念は受け継がれ、私たちが目の当たりにしている世界的な自由運動を後押ししています。

毎日、一般の人々が法定通貨システムから抜け出し、ビットコインの世界へと足を踏み入れているのです。

自由を求める人々によって、世界中のさまざまな地域でビットコインハブ、いわゆるビットコイン循環経済が立ち上げられています。

エルサルバドルのように、新たな道を模索している国でさえも、独自の方法でビットコインの導入を始めています。

6.1 ビットコインはどのように機能するのか？

6.1.1 ナカモト・コンセンサス・メカニズム

では、ビットコインはどのように機能するのでしょうか？ビットコインには多くの機能があり、その仕組みはまるでウサギの穴のように、奥がとても深いのです。

とはいって、ビットコインの世界に初めて足を踏み入れる場合、使い始めるために仕組みを完全に理解する必要はありません。

これはインターネットを使うときと同じです。ほとんどの人はTCP/IPプロトコルの仕組みを知りませんが、毎日メールを送ったり、メッセージをやりとりしたり、SNSに投稿したりしています。

車を運転するのも同じです。多くの人は車の構造を正確には理解していませんが、運転の仕方は知っています。



しかし、ビットコインはまだ広く普及していません。1990年代のインターネットのように、まだ比較的新しいテクノロジーです。そのため、ビットコインの基本的な仕組みをなるべくシンプルに、技術的でない形で理解しておくと役立つでしょう。

第6章

ビットコインの仕組みの核心を一言で要約すると、
「ビットコインはオンライン上の人々の合意」であると言えます。

友だちとボードゲームをするようなものだと考えてみてください。モノポリーのようなゲームでは、参加者全員がルールに同意しています。例えばモノポリーのルールでは、特別な「モノポリーのお札」しか使えません。

もしプレイヤーの1人であるジェームズが、ルールに反してトイレットペーパーで家を買おうとしたら、他のプレイヤーは彼をズルだと指摘し、一緒にプレイするのをやめるでしょう。

要するに、そのゲームに参加するためには、お互いにルールを共有し、そのルールから逸脱しない必要があります。そうでなければ排除されます。

これはビットコインの根本的な仕組みです。ビットコインは、同じ一連のルールに合意する人々のネットワークです。これらのルールは数学的に結び付けられ、コンピュータコードで記述され、ビットコインソフトウェアを実行するすべての人によって直接受け入れられています。

ビットコインのルールはすべての参加者に平等に適用されます。
つまり、誰もがゲームのルールに従うか、さもなければネットワークに拒否されてプレイできないかのどちらかです。

例えば、ビットコインのルールの1つに「ビットコインの総発行数は2,100万枚を超えない」というものがあります。

もし誰かが自分用に100万枚のビットコインを余分に作り出そうとしても、それは無意味です。

なぜなら、そのビットコインは自動的に他の参加者によって識別され、拒否されるからです。

これがビットコインの堅牢性を支えています。

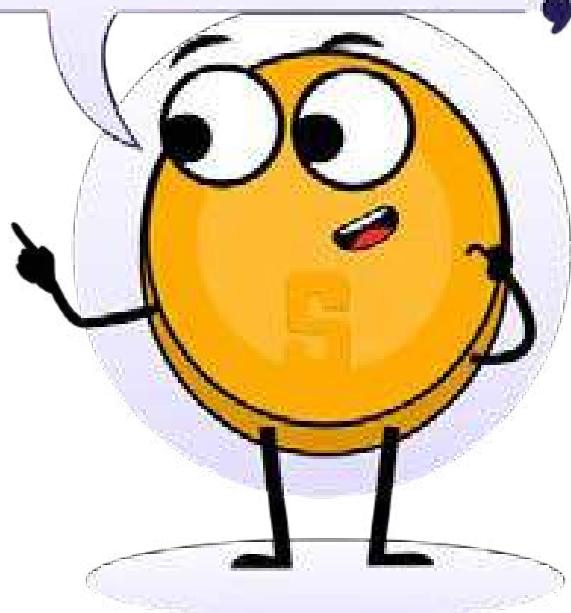
あなたが誰であろうと、どこから来た人であろうと関係ありません。ビットコインの世界に入るなら、他の人と同じルールに従う必要があります。

この原則は、法定通貨の世界で絶大な権力や影響力をを持つ、すべての人々や組織にも当てはまります。

ビットコインの世界には、不正行為や妨害の余地はなく、誰もが平等に扱われ、それを変えることは誰にもできません。

知ってた？2009年から今まで、ビットコインは何万回ものハッキングや改ざん、変更の試みに耐えてきたんだよ。

ビットコインは誰にも止められないし、支配も操作もできないってことを証明しているんだ！



ビットコイン入門

6.1.2 ゲームプレイヤーたち

ビットコインの分散性をより深く理解するためには、ネットワーク内のさまざまな役割について掘り下げる必要があります。

ビットコインの世界では、さまざまな参加者が、それぞれ異なる役割を果たしながらも調和を保ち、ネットワークの円滑な機能を支えています。

1.マイナー：セキュリティの設計者

マイナー（採掘者）はビットコインの基盤です。

彼らは個人またはグループであり、プルーフ・オブ・ワーク（PoW）と呼ばれる仕組みを通じてネットワークの維持と保護を担っています。

マイナーは高い計算能力を持つ特別なコンピューターを使用します。

彼らはビットコインネットワークに自分のハードウェアを提供し、世界規模の“くじ引き”のような仕組みで競い合い、ビットコインの分散型台帳（ブロックチェーン）に新しいトランザクションブロックを追加するのです。

彼らの献身的な取り組みによって、台帳の不变性が保たれ、悪意ある攻撃からネットワークが守られます。



マイニングは分散型であるため、十分な計算リソースがあれば誰でも参加可能です。最も早くパズルを解いたマイナーには、報酬としてビットコインが与えられます。

ビットコインマイナーは世界中に分散しており、ネットワークの中央集権化を防ぎながら、強固で分散的なセキュリティを維持しています。

2.ノード：検証の門番

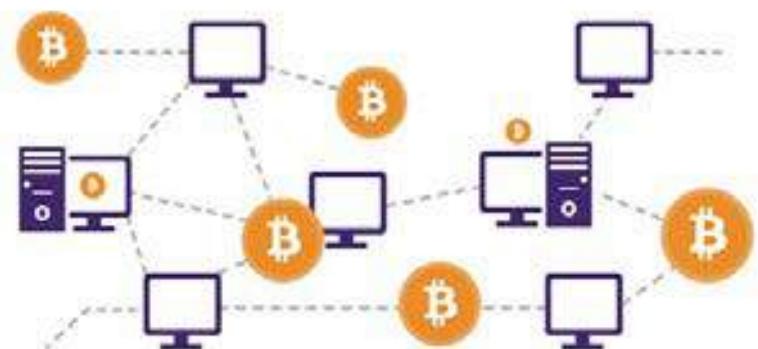
ビットコインノードは、世界中に住む一般の人々です。

彼らは小型コンピューター上でビットコインソフトウェアを実行し、台帳全体のコピーを維持することで、ビットコインネットワークの門番としての役割を果たしています。

ノードはトランザクションを検証し、すべての参加者がコンセンサスルール（合意のルール）に従っているかを確認します。

検証の責任をノードのネットワーク全体に分散させることで、ビットコインは攻撃に対する耐性を保ち、信頼に頼らない仕組みを維持できるのです。

ノードは台帳の整合性を守る重要な役割を担っており、ビットコインの分散化という理念に大きく貢献しています。



第6章

ユーザー：自立した参加者

ユーザーはビットコインネットワークの生命線であり、実際に取引を行う人々のことです。彼らは日々の暮らしを送りながら、ビットコインを導入することで自分自身に力を与えています。

例えば、ビットコインでお金を貯蓄するユーザーもいれば、エルサルバドルの市民のように、食料品を購入したり給与を受け取ったりするためのお金としてビットコインを使用するユーザーもいます。

ビットコインは、銀行や政府といった仲介者を排除し、直接的なピア・ツー・ピア取引を可能にすることで、ユーザーに力を与えます。

つまり、ユーザーはお金と取引をすべて自分で管理できるようになります。

開発者とプロジェクト：イノベーションの設計者

未来の金融システムは独力で築かれるものではなく、努力なしに倫理的に正しい方法で世界中に採用されることもありません。そこで登場するのが、ビットコインの開発者やプロジェクトです。

開発者たちは技術的な専門知識を生かし、ビットコインのプロトコルを強化・革新します。彼らはコードの提供・改善提案・脆弱性への対応を行い、ネットワークがあらゆる課題に対応しながら進化していくよう支えています。ビットコインはオープンソースであるため、世界中の開発者が協力し、成長に貢献することができるのです。

この分散型開発の素晴らしさは、単一の主体がプロトコルを独占的に支配することを防ぐ点にあります。これはコンセンサス（合意形成）主導のプロセスを通じて行われます。

開発者がアイデアや変更を提案し、より良い世界というビジョンと一致する優れた提案だけが、コミュニティからの支持を受けて採用されるのです。

こうしてビットコインは、80億人規模の利用に向けて透明で民主的な進化を遂げていきます。

ビットコイン関連のプロジェクトには、目的意識を持つ非営利団体や企業、価値あるコンテンツを生み出す個人やグループなど、多様な人々が関わっています。

彼らは「集団的の自由」という大きなビットコインの使命の一部として、それぞれ特定の目標や分野に取り組みながら協力しています。

これらのプロジェクトは、ビットコインの採用を形成・促進する上で重要な役割を果たし、人類のエンパワーメント（力を与えること）と自由を優先する未来を目指しているのです。

シンフォニー

ビットコインの分散性は、相乗効果を生む音楽オーケストラに例えることができます。すべての演奏者がバランスを保つつつ、美しい音楽を奏でているのです。

ビットコインネットワークにはボスは存在しません。その代わり、マイナー・ノード・ユーザー・開発者・プロジェクトが、それぞれ自律性と協調性をもって役割を果たしています。

ノードによって維持される分散型台帳は透明性を保証し、PoWメカニズムはセキュリティを提供し、マイニングの中央集権化を防ぎます。

ユーザーは、法定通貨システムの支配から解放され、金融的主権とエンパワーメントを体験します。

開発者はコンセンサスに導かれながら、プロトコルを人類のニーズに応じて進化させていきます。

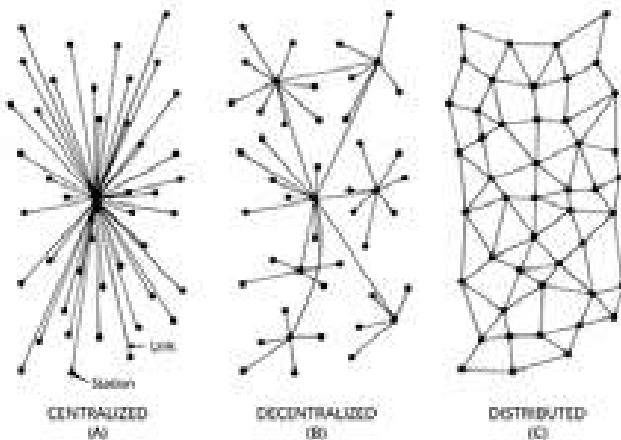
プロジェクトはそれぞれ独自の方法で、集団的な自由という大きな目標に貢献しています。

ビットコイン入門

見ての通り、すべての参加者がビットコインの普及と人類のエンパワーメントにおいて、重要な役割を担っています。

この分散型オーケストラの各参加者が、ビットコインの回復力と持続可能性に貢献し、信頼不要で国境を越えた、人々を力づけるエコシステムを形作っています。

要するに、ビットコインにおける分散性のシンフォニー（交響曲）は、サトシ・ナカモトのビジョンと、自由とエンパワーメントを追い求める世界中のコミュニティによる、計り知れない情熱の証として響き渡っているということです。



クラス演習 – ピア・ツー・ピア (P2P) ネットワークにおける合意形成



目的：

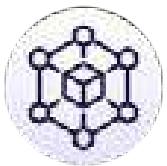
グループ内で合意がどのように形成されるかを理解し、ビットコインにおける暗号技術とコンセンサスレイヤーについて学ぶ。



必要なもの：

以下のメッセージが書かれた紙

- ・「ATTACK (攻撃)」(暗号化されていないメッセージ)
- ・「4-16-14-21-1-21-21-1-3-11-」(暗号化されているメッセージ)



準備：

先生は授業前に3~4人の生徒を選び、「悪意あるノード」として指定しておきます。これらの生徒には、前の授業で暗号の変換方法を宿題として伝えておきます。

第6章

演習手順：

1

先生はグループの中から1人の生徒を「発信者」として選びます。
その生徒には「ATTACK (攻撃)」「4-16-14-21-1-21-21-1-3-11-」と書かれた紙が渡されます。

2

生徒たちは指定されたスペースに円を作って並びます。
「悪意あるノード」に指定された生徒たちは離れた位置になるようにして、演習の効果を高めます。



3

グループが円形に並んだら、「発信者」は紙を右隣の人へ渡します。

4

全員がメッセージを読んだ後、こう伝えます：
「メッセージが“ATTACK (攻撃)”だと思ったら、発信者が合図したタイミングで一步前に出てください。ただし、メッセージをどう解釈するか、どう行動するかは各自の判断に任せます。」
発信者が「せーの！」と声をかけて合図を出します。
メッセージが「ATTACK (攻撃)」だと判断した参加者は、前に一步踏み出します。

5

暗号化されたメッセージを受け取り、それを正しく解読できた一部の生徒の中には、動かずしてその場にとどまる者も出てきます。
一方、それ以外の生徒たちは「ATTACK (攻撃)」という指示に従うため、グループ内で合意（コンセンサス）が形成されていないことが明らかになります。

まとめ：

コンセンサスがなぜ成立しなかったのかを話し合い、「ビザンチン将軍問題」という概念を紹介します。
その上で、共通の目標の必要性について説明し、最終的にこの問題に対するビットコインの解決策について議論します。

ビットコイン入門

6.2 健全なデジタルマネーとしてのビットコイン

6.2.1 はじめに

アクティビティ：

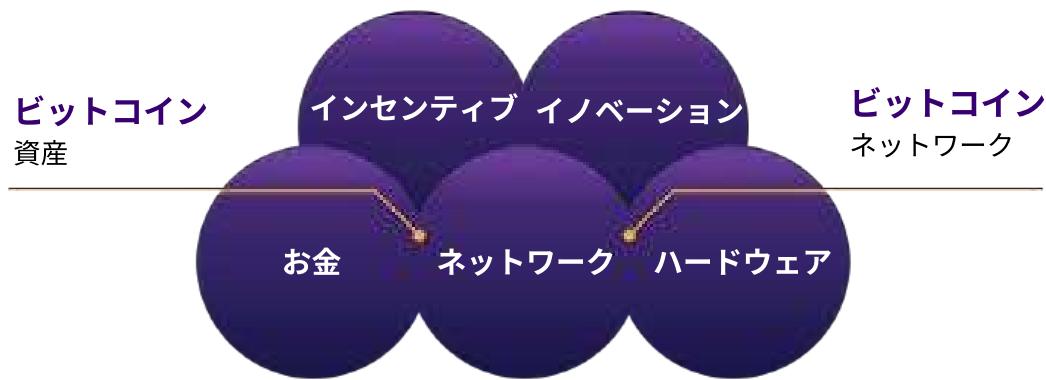
1分半の動画
「What Is Bitcoin?
(ビットコインとは何か)」を
見てみよう！



簡単に言えば、ビットコインはお金です。
ビットコインは投資ではなく、
苦労して稼いだお金を安全に、力強く貯蓄
する手段です。

ビットコインを持っていても、
それ自体で富を築くわけではありません。
ビットコインが追加で増えるわけではないからです。

その価値は法定通貨と比べて上昇すること
はあります、それは主にビットコインの
普及が進んでいることと、
法定通貨の価値下落によるものです。



ビットコインは新しい形のお金であり、「お金のインターネット」です。これは、誰でも参加し、他のユーザーと
価値の交換を始められることを意味します。

これまで孤立していた貧しい地域の人々も、ついに金融システムにアクセスできるようになりました。

電話とインターネット接続さえあれば誰でも検索エンジンを使えるように、
ビットコインは電話とインターネット接続があれば誰でも、新しいグローバルな金融システムにアクセスできる
ようにします。



より速く、
より安い送金



金融包摶



プライバシーの
向上

数分で世界中に送金可能、
手数料は極めて低い。

銀行口座を持たない25億人が、
電話やパソコンを通じてお金へ
アクセスできる。

ビットコインの取引は
公開されるが、
あなたの身元は公開されない。

第6章

ビットコインは完全にデジタルであり、
国境がありません。
世界中のコンピューターやスマートフォン上
に存在するため、
あなたがどこにいるかは関係ありません。
世界中の多くのユーザーが、ビットコインの
ソフトウェアと台帳のコピーを
実行しています。

このソフトウェアとすべての取引記録は、
数えきれないほどのコピーが存在するため、
消滅する可能性は非常に低いです。

もしそれを停止させたいなら、
インターネット全体を永遠にシャットダウン
する必要がありますが、そのようなことが
起こる可能性は限りなく低いでしょう。

最後に、ビットコインは希少です。
存在できるビットコインの数には絶対的な上限があります。
ビットコインを偽造することは誰にもできません。
最も強力な政府や金融機関でさえも、それは不可能です。



6.2.2 ビットコインの特徴

健全な通貨の進化

第2章で学んだように、健全な貨幣のライフサイクルは、社会から広く受け入れられるために3つの段階を経て進行します。

それは、まず「価値の保存手段」から始まり、次に「交換の媒介手段」、最後に「計算単位」になるという流れです。

通貨の最初の段階である「価値の保存手段」は、通貨が時間とともに安定した（もしくは価値が上がる）資産として信頼され始める時期です。

この特徴に早く気づいた人々は、特に地政学的・マクロ経済的に不安定な時期に、自分の資産を守るためにこのような通貨に換えて貯蓄しようとします。

一部のメディアなどは、ビットコインを「デジタル・ゴールド」と呼んでいます。

それは、ビットコインが過去10年間で「価値の保存手段」としての地位を確立したからです。

毎日、ますます多くの人々が、ビットコインをインフレに対するヘッジ（資産防衛手段）としてとらえ始めています。これは、歴史的に金（ゴールド）が担っていた役割と同じです。

次の段階は、通貨の安定性に対する信頼がより強固になる時期です。

この段階では通貨が「交換の媒介手段」として機能し始め、人々の日常生活における取引を促進します。
そしてモノやサービスとの交換手段として、広く受け入れられるようになります。

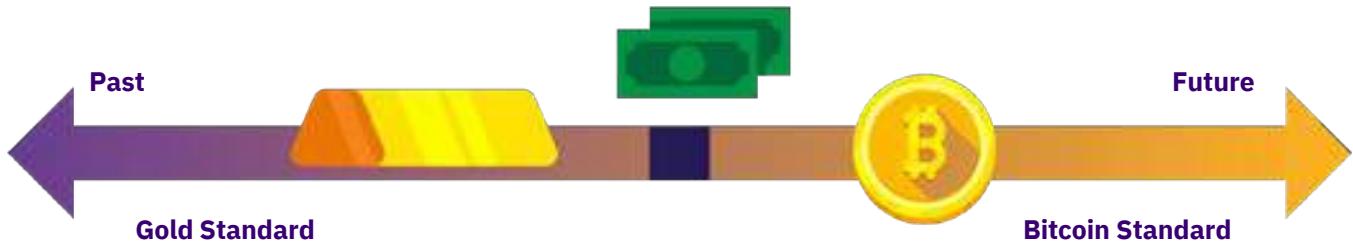
ビットコインは、交換の媒介手段へと着実に移行しています。

加盟店の増加やプロトコルの発展により、ビットコイン取引は日常の商取引において、より効率的かつ一般的になりつつあるのです。

その一例がエルサルバドルで、同国ではビットコインが法定通貨の1つとして扱われています。

今では、世界中で多くの一般市民や企業が、ビットコインを交換の媒介手段として利用しています。

ビットコイン入門



最終段階では、通貨は「計算単位」としての地位を確立し、モノやサービスの価格を示す共通の尺度として機能します。

この段階に至ると、その通貨は他のすべての価値を測る標準的な指標となります。

計算単位になるまでの道のりは、より長期的なプロセスです。現在、世界ではモノやサービスの価値は法定通貨で測られており、ビットコインがこの段階に到達するには、さらなる普及と金融システムへの統合が必要です。

しかし、すでにその土台は築かれつつあります。

企業や個人がビットコインで価値を考えたり、価格を表示したりし始めているからです。



見ての通り、ビットコインは健全な通貨としての進化のサイクルを着実に進んでいます。

ビットコインがグローバルな金融システムに完全に統合されれば、標準的な計算単位となり、世界の通貨システム全体を再構築する可能性があります。

第6章

お金の特性

第2章で学んだように、人類は長い時間をかけて、「真に健全なお金」はある特定の性質を持っている必要があると理解するようになりました。

その性質とは、耐久性・分割可能性・携帯性・受容性・希少性・均一性です。

では、ビットコインがこの基準を満たしているかを見ていきましょう。

耐久性：

ビットコインは純粋にデジタルな存在であり、完全に耐久性があります。物理的に劣化しません。

分割可能性：

比較として挙げると、法定通貨である米ドルはセント（0.01）まで分割できます。

ビットコインは「satoshi」または「sat」（0.00000001）という最小単位にまで分割可能です。

そして、ビットコインはデジタルな性質を持つため、将来人類が必要とすれば、さらに細かく分割することもできます。

現在、ビットコインは世界で最も分割性の高い金融資産です。

携帯性：

2020年4月、11億ドルがわずか数分で送金され、かかった手数料はたったの68セントでした。
他の支払い方法では、これほど低コストで迅速に、しかも中央管理者なしでこれほどの大金を移動させることはできません。

これが、ビットコインが世界で最も簡単に移動できるお金である理由です。

受容性：

ビットコインは交換手段としてはまだ初期段階にあり、法定通貨と比べると、受け入れられ度合いは低いのが現状です。

希少性：

ビットコインは、2100万枚しか存在しません。

この数量を増加させることはコードによって不可能であり、これにより、ビットコインは希少であるだけでなく、比類なき希少性を持つ金融資産でもあるのです。

均一性：

均一性：ビットコインの各単位は、他のどの単位とも等しく交換可能であり、
ビットコイン・プロトコル上で同種のものとして交換や取引ができます。
この性質が、ビットコインを代替可能な通貨にしているのです。

ビットコイン入門

ビットコイン vs. 金（ゴールド） vs. 米ドル

お金の特性	金	米ドル	ビットコイン
耐久性	高	中	高
携帯性	中	高	高
分割可能性	中	中	高
均一性	高	高	高
希少性	中	低	高
検証可能性	中	中	高
確立された歴史	高	中	低
検閲耐性	中	中	高
スマート／プログラム可能性	低	中	高

"Bitcoin vs Gold vs US Dollar" Bitcoin Magazine, <https://bitcoinmagazine.com>

ビットコインは、プログラム可能で、没収されることがなく、貯蓄に適していて、迅速な取引を望む商人にとって使いやすい、さまざまな性質を備えたスマートマネーの一種です。

透明なデジタル台帳であるため、ビットコインはネットワーク上での詐欺の発見やリスクの特定において、非常に効率的になります。

限られた量しかないという金の利点を持ちながらも、法定通貨のように細かく分割でき、持ち運びも簡単です。

さらに、現代のデジタル社会に適した新しい機能も備えています。

どう思いますか？ビットコインはまだ広く認識・採用されているわけではありませんが、健全な通貨と言えるでしょうか？

第6章

アクティビティ：クラスディスカッション——ビットコインは「健全なお金」か？

ビットコインについて詳しく学んだところで、第2章にあった「お金の比較表」をもう一度見てみましょう。ビットコインは他の形態のお金と比べてどうでしょうか？

良いお金の特性	牛	紙巻たばこ	ダイヤモンド	ユーロ	ビットコイン
耐久性					
携帯性					
均一性					
受容性					
希少性					
分割可能性					
合計					

6.2.3 自己責任を受け入れる



その結果、単一障害点のない分散型システムが実現した。
ユーザーは自分自身で暗号鍵を管理し、P2Pネットワークの支援によって二重支払いをチェックしながら、互いに直接取引する。

サトシ・ナカモト



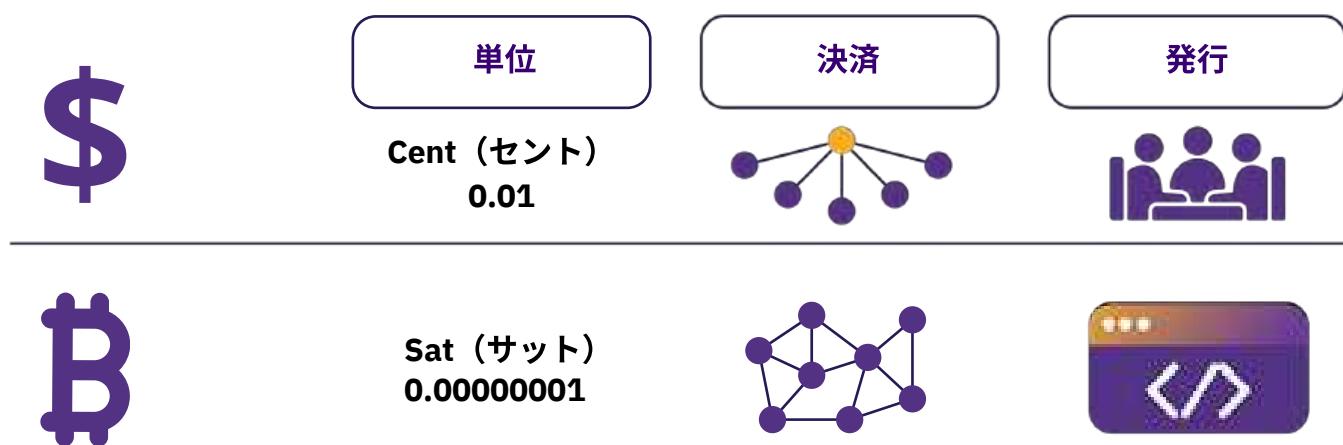
ビットコイン入門

法定通貨の世界では、人々は政府、銀行、そして既存の決済プロバイダーに依存しています。これらの（金融）機関の上層部がネットワークのルールを定め、その参加者である一般市民の多くはルールに従わなければなりません。どこに住んでいようと関係なく、何をどうすべきかを示す標準的な手順が必ず存在します。こうした仕組みは、特に日々生活での課題が増大する家庭にとって、長年にわたって苦難の連鎖を生んできました。

人々はこのような仕組みのもとで、自分のお金の責任を他人に委ねることが当たり前になっています。例えば、多くの人は何か問題が発生した時（銀行口座へのアクセスを失うなど）、誰かに助けを求めるます。



ご存じのとおり、ビットコインの金融システムは大きく異なります。ビットコインは特定の仕組みで動作し、支配者は自律的なルールシステムに置き換えられました。独裁者もリーダーもないため、何をすべきかを誰かに命令されることはありません。もしビットコインがもたらす新たな自由と力を得たいのなら、その仕組みを理解し、自分に合った方法でその技術を取り入れる必要があります。



第6章

ビットコインにおいては、自分の資産を完全に自分で管理できますが、その分責任も大きくなります。例えば、デジタルウォレットの管理を誤り、秘密鍵を失ってビットコインにアクセスできなくなると、その貯蓄は永久に失われてしまいます。困ったときに電話できるカスタマーサービスも、頼れる人もいません。問題が起きた時は、自分で対応する必要があるのです。

幸いなことに、自分の人生に対して完全に責任を負うと決めた人にとっては、こうした事態は起こりません。ビットコインを使うこと自体は特別に難しいわけではなく、単に新しい概念であるだけです。不慣れなために生じる不便さはありますが、ビットコインの使い方を学び、自分の資産を守る責任を完全に受け入れる意欲があれば、ビットコインは非常に強力なツールとなります。あなたは資産のコントロールを握り、誰にも奪われることはありません。

要するに、鍵となるのは「行動すること」であり、ビットコインの仕組みを理解し、自分自身のニーズや人生観に沿って取り入れていくことです。

次の章ではビットコインウォレットを作成します。初めての送金と受け取りを行い、セキュリティの最良の事例を確認しましょう。

第7章： ビットコインの 使い方

7.0 はじめに

7.1 ビットコインの入手と交換

7.1.1 P2P：対面での取引

7.1.2 P2P：オンラインでの取引

7.1.3 中央集権型取引所

7.2 ビットコインウォレット入門

7.2.1 セルフカストディ型ウォレットvsカストディ型ウォレット

7.2.2 ビットコインウォレットの種類

7.2.3 オープンソースvsクローズドソース

アクティビティ： bitcoin.orgでのビットコインウォレットの評価

7.3 モバイルビットコインウォレットの設定

アクティビティ：ウォレットの設定／復元

7.4 受け取りと送金の方法

アクティビティ：ビットコイン送受信の実践

7.5 ビットコインで貯蓄する

7.6 Don't Trust, Verify - 信じるな、検証せよ

生徒用ワークブック

日本語版 | 2025年版

ビットコインの使い方

7.0 はじめに

「一体なぜ中央銀行マネーに対抗して「オタクマネー」を信頼するのかって？
オタクは皆にインターネットをもたらした。
銀行が皆にもたらしたもの、それは大恐慌だ。」

アンドレアス・M・アントノプロス

ビットコインとは何か、そしてその目的について理解が深まったところで、今度は実際に使う方法を学んでいきましょう。

この章では、ビットコインを手に入れる手順を段階的に紹介し、利用できるウォレットの種類を解説し、あなた自身のビットコインウォレットの設定をサポートします。

さらに、ネットワーク上のビットコイントランザクションの送受信と追跡を練習します。

理解を行動に変えるときが来ました！

7.1 ビットコインの入手と交換

ビットコイン入手する方法はいくつもあります。

例えば、以下のような方法があります：

- ◆ 仕事の対価としてビットコインを受け取ったり、他の人々の製品やサービスの支払いをビットコインで行ったりする（第8章で解説）
- ◆ ビットコインをマイニングする（第9章で解説）
- ◆ 法定通貨をビットコインに交換する、またはその逆を対面で行う
- ◆ 法定通貨をビットコインに交換する、またはその逆をオンラインで行う



以下では、最も一般的な選択肢である対面取引とオンライン取引の両方を通じて、法定通貨とビットコインの交換について掘り下げていきます。

7.1.1 P2P：対面での取引

ピア・ツー・ピア（P2P）取引を通じてビットコインの売買を行う場合、銀行やその他の第三者を介さずに、個人同士で法定通貨（または他の商品やサービス）とビットコインを直接交換します。

両当事者の合意のもと、交換する金額やレートを決定します。

買い手が現金を渡し、売り手がビットコインを送信することで取引成立です。

P2P取引は、現実世界で相手に直接会って行う方が簡単ですが、インターネットのおかげで事実上どこからでも行えます。

また、ビットコインを法定通貨に交換する場合は、これと同じ手順を行います。



第7章

7.1.2 P2P：オンラインでの取引

P2Pプラットフォームが登場し、ビットコインの買い手と売り手がサイバー空間で直接取引できるようになりました。仲介者を介さず、インターネット上で直接取引を行えます。

このようなプラットフォームを使えば、自分の情報やお金を誰かに預ける必要はありません。
他のユーザーと直接つながって取引できます。



ほとんどのP2Pプラットフォームでは、取引相手同士が約束を守ることを保証するために、資金の一部をエスクローする必要があります。

エスクローとは、両当事者が約束を果たし終えるまで、プラットフォームが管理する安全な場所に資金を置くことを意味します。

例えるなら、信頼できる友人が、みんなが約束を守るまで一時的に預かってくれるような仕組みです。

翻訳者注釈：

現在もP2Pプラットフォームは存在しますが、日本では規制の影響もあり利用者は少なく、リスクの高い手段とされています。一方で、国や地域によっては、こうした手段が非常に重要な役割を果たしていることもあります。

7.1.3 中央集権型取引所

中央集権型取引所とは、ユーザーがその企業を通じて直接ビットコインの売買を行えるサービスのことです。取引所の利用はビットコインの売買を最も簡単に行う方法の1つですが、利便性にはコストを伴うなど、大きなトレードオフ（代償）もあります。

中央集権型取引所とそのトレードオフ



CENTRALIZED

中央集権型取引所でビットコインを購入する場合、本人確認のために個人情報の提供が求められるのが一般的です。

これにより、個人情報の盗難リスクや外部からの潜在的な脅威にさらされる可能性があります。

さらに、取引所はユーザーのビットコインを預かるため、ビットコインを自分で引き出すまでは、自分自身で資産を管理しているとは言えません。

そして、取引所によっては、ユーザーの資金を不正流用したり、保有していない以上のビットコインを貸し出したりすることもあり、最終的には破綻に至るケースもあります。

……そう、まるで銀行のように！

しかしビットコインの世界には、不正な銀行を救済するために通貨を増刷する中央銀行はありません。ビットコインは刷れないので。

ビットコインの使い方

7.2 ビットコインウォレット入門

ビットコインは物理的なお金とは異なり、ウォレットの中に実際に存在しているわけではありません。

代わりに、ビットコインネットワークが常に検証し、保護している分散型台帳上に存在します。

では、どのようにしてビットコインを所有できるのでしょうか？

あなたがビットコインの所有権を持つのは、取引に署名し、ビットコインの所有権を他者に移転するための秘密鍵を所有している場合のみです。これが、ビットコインを送るという行為です。

このことを踏まえて、「ウォレット」という言葉が意味する2つの概念を見ていきましょう。



- ✿ マスター秘密鍵（パスワードのようなもの）：これを使って、ビットコインを受け取ったり送ったりするために他者と共有できる公開鍵を生成できます。
- ✿ モバイルまたはデスクトップのインターフェース：これを通じてビットコインネットワークとやり取りし、ビットコイン残高の取得・送金・受け取りや、ネットワークへのブロードキャスト（公開送信）ができます。

7.2.1 セルフカストディ型ウォレット vs カストディ型ウォレット

ビットコインウォレットの種類や特徴を詳しく説明する前に、以下の表で示されているように、セルフカストディ型ウォレット（自己管理型ウォレット）とカストディ型ウォレットの重要な違いを確認しましょう。

それぞれのウォレットタイプの利点とリスク、そして誰がビットコインを管理するのかが分かります。セルフカストディ型はユーザー自身が秘密鍵を保持し、ビットコインを本当の意味で所有する状態です。一方、カストディ型ウォレットは第三者がビットコインを保持します。

ウォレットの種類	誰がビットコインを管理するのか	利点	リスク
セルフカストディ型ウォレット	ユーザー自身	<ul style="list-style-type: none">・資金や取引を完全にコントロールできる・承認プロセスなし／アカウント凍結なし・企業や政府の支配なし・恣意的な没収から保護される (自宅に現金を保管するのと同様)	<ul style="list-style-type: none">・リカバリーフレーズを失うと復元できない・カスタマーサポートが少ない・すべての責任はユーザー自身にある
カストディ型ウォレット	第三者の事業者	<ul style="list-style-type: none">・アクセスを失っても簡単に復旧できる・カスタマーサポートが受けやすい	<ul style="list-style-type: none">・常にインターネットに接続されているため、ハッキングや情報漏洩のリスクがより高い・カストディアン（管理業者）が口座を管理し、アカウントを凍結する権限を持つ

第7章

セルフカストディ型ウォレット（ノンカストディアルウォレットとも呼ばれる）では、秘密鍵を持っているのはあなただけで、資金の出し入れを完全に自分でコントロールできます。

一方、カストディ型ウォレットでは第三者が秘密鍵を保持しており、その人があなたの代わりにビットコインを動かす完全な権限を持っています。

 セルフカストディ（自己管理）とは、自分自身が銀行になるようなものです。取引は政府や企業によるコントロールや権限の対象にはなりませんが、同時にビットコインを安全に保つ全責任を負うことを意味します。

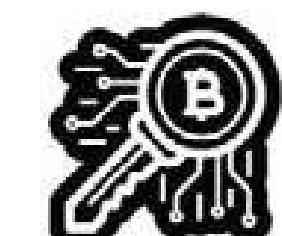
 セルフカストディであれば、第三者があなたの同意なくビットコインを没収することはできません。

 セルフカストディは、不確実な時代においても、自分のビットコインが安全であるという安心感を与えてくれます。

個々のニーズに合う、適切なウォレットの種類を選ぶことが重要です。

ただし、セルフカストディ型かカストディ型か、インストール時に見分けがつきにくいこともあります。以下の表は、インストールの流れと違いを示したものです。

ウォレットのタイプ	ステップ1：ウォレットを選ぶ	ステップ2：ウォレットをインストール	ステップ3：新しいウォレットを作成	ステップ4：リカバリーフレーズを保管	ステップ5：ウォレットの使用開始
セルフカストディ型ウォレット	セルフカストディ型ウォレットプロバイダー(提供元)を選ぶ	ウォレットプロバイダーの指示に従う	リカバリーフレーズと最低1つの秘密鍵を生成	リカバリーフレーズを安全な場所に保管する	ウォレットを使ってビットコインの受け取り・送信を始める
カストディ型ウォレット	カストディ型ウォレットプロバイダー(提供元)を選ぶ	ウォレットプロバイダーの指示に従う	ウォレットプロバイダーでアカウントを作成	該当なし (秘密鍵はウォレットプロバイダーが管理)	ウォレットを使ってビットコインの受け取り・送信を始める



NOT YOUR KEYS
NOT YOUR COINS

「Not your keys, not your coins（あなたの鍵でなければ、あなたのコインではない）」これはビットコイン保有者の間でよく知られている言葉です。

この言葉は、ビットコインウォレットに関連付けられた秘密鍵を自分で直接管理していない場合、そのビットコインを真に所有しているとは言えない、という考え方を表しています。

秘密鍵にアクセスできる者は誰でも、あなたのビットコインの所有権を得てしまします。

そのため、秘密鍵を他人の目から遠ざけて守ることが最も重要なのです！これを実現する方法については、本書の後半でいくつか紹介します。

ここから先は、ユーザー自身が鍵を所有し、ビットコインを完全にコントロールできるセルフカストディウォレットを取り上げていきます。

*難しく感じたり、全部を理解できなかったりしても、心配しなくて大丈夫です。

これは旅のようなもので、ビットコインを使い始めていけば、だんだんわかってきます！

ビットコインの使い方

7.2.2 ビットコインウォレットの種類

秘密鍵の作成および保管場所によって、ビットコインウォレットにはさまざまな名前が使われます。

スマートフォンに鍵が保存されている場合は「モバイルウォレット」、

専用のデバイスに安全に保存されている場合は「ハードウェアウォレット」、

紙にのみ鍵が保存されている場合は「ペーパーウォレット」と呼ばれます。

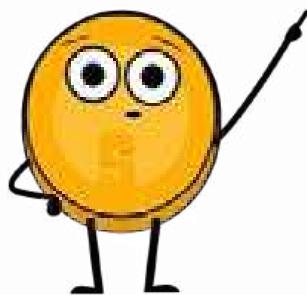
ウォレットの構造によって異なる名称：

ウォレットタイプ	説明	利点	欠点	ユーザーの例
オンラインウォレット	Webブラウザからアクセスするウォレット	インターネット接続があればどのデバイスからでもアクセス可能／使いやすい	セキュリティが低い／ハッキングや情報漏洩のリスクあり	頻繁にウォレットにアクセスする必要があり、多額の資金を保管しない人
モバイルウォレット	モバイルデバイスにインストールされたウォレット	利便性が高い／どこからでもアクセス可能	デバイスの紛失、盗難、ハッキングによりアクセスできなくなる可能性あり	外出先で取引する必要があり、多額の資金は保管しない人
デスクトップウォレット	デスクトップPCにインストールされたウォレット	オンラインウォレットよりも安全／オフラインで使用可能	マルウェア感染などによりハッキングされるリスクあり	多額のビットコインを保管したいと考えており、PCの使用に慣れている人
ハードウェアウォレット	ビットコインをオフラインで保管する物理デバイス	非常に安全／オフラインで使用可能	デバイスの紛失や盗難により、資金が回復不能になる可能性あり	多額のビットコインを保管したいと考えており、追加のセキュリティのために費用をかけられる人
ペーパーウォレット	ビットコインウォレットの秘密鍵と公開鍵を記載した物理的な記録	非常に安全／オフラインで使用可能	物理的な記録の紛失や盗難によって、資金が失われる可能性あり	多額のビットコインを保管したいと考えており、セキュリティ向上のために多くの予防策を講じたい人

第7章

ビットコインウォレットの秘密鍵は、あるデバイスから別のデバイスにインポートできるため、そのウォレットがどのタイプに分類されるかは使い方によって変わります。

例えば、パソコン上で秘密鍵を生成し、それを後にスマートフォンにインポートした場合、「デスクトップウォレット」が「モバイルウォレット」として利用されるようになります。



ビットコインを保管する時は、「誰が管理しているか」だけじゃなくて、他にもたくさんのリスクについて考える必要があるんだ。
だからこそ、安全で便利な保管方法を見つけるのが大事だよ。

いろんな種類のウォレットを比べてみると、すべてのニーズを完璧に満たしてくれる理想的なウォレットは存在しないってことがわかってくるよね。

ビットコインウォレットを選ぶときには、いくつかの点を考慮する必要があります：

- ◆ **セキュリティ：** 二要素認証や安全なパスワードポリシーなど、強固なセキュリティ対策が講じられているかを確認しましょう。
- ◆ **プライバシー：** 匿名性を保てるか、それともアカウント作成に個人情報が必要かを考慮してください。
- ◆ **使いやすさ：** 特に初心者の場合は、操作が簡単で分かりやすいウォレットを選びましょう。
- ◆ **互換性：** 自分のデバイスやOSに対応しているかどうか確認してください。
- ◆ **手数料：** ウォレットごとの手数料を比較して、最も条件がよいものを選びましょう。
- ◆ **評判：** ウォレットや開発チームの評判を調査し、信頼できるか調べてください。
- ◆ **管理権限：** 秘密鍵をどの程度自分で管理できるかを確かめます。
自分で管理できればセキュリティ上の利点となる場合があります。

「完全に自分で管理するウォレット」が良いか、「使いやすいけれど自己管理は限定的なウォレット」が良いか、じっくり考えて選びましょう。

7.2.3 オープンソース vs クローズドソース

ビットコインウォレットを選ぶ際にもう一つ重要なのが、そのアプリやソフトウェアがオープンソースかどうかを確認することです。

オープンソースコードは、コミュニティがコードをレビューでき、チームが作業を中止した場合でもプロジェクトの開発を継続できるため、非常に重要です。

ビットコインの使い方



ビットコインのコードが誰でもレビュー・使用・変更できる完全なオープンなものであるのと同じように、ビットコインを保管するウォレットのコードもオープンであるべきです。

アクティビティ：bitcoin.orgでのビットコインウォレットの評価

以下のウェブサイトにアクセスしてください：
<https://bitcoin.org/en/choose-your-wallet>

今回学んだウォレットの知識を活かし、評価基準に基づいて最適なウォレットを選びましょう。



7.3 モバイルビットコインウォレットの設定

ビットコインウォレットとそれらの違いについて理解を深めたところで、実際にウォレットを使用する方法を見ていきましょう。この例では、スマートフォン上に直接モバイルウォレットを作成します。

アクティビティ：ウォレットの設定／復元

もし生徒が携帯電話を持っていない場合は、先生が貸し出します。
このアクティビティには2つの選択肢があります。

第7章

クラス演習：選択肢1 – 新しいウォレットをダウンロードする



ビットコインウォレットの作成と使用方法：

- 1 App Store (iOS) またはGoogle Playストア (Android) でアプリを検索します。
- 2 アプリを開き、画面の指示に従ってウォレットの新規作成を進めると、12語または24語のリカバリーフレーズ（シードフレーズと呼ばれることがあります）が生成され、表示されます。これを必ず紙などに書き留め、安全な場所に保管してください！リカバリーフレーズがあれば、必要に応じて資金へのアクセスを完全に回復できます。
- 3 この単語の並びを紛失したり忘れててしまうと、ウォレットへのアクセスを失った場合にビットコインにアクセスできなくなることを忘れないでください。
- 4 次に、リカバリーフレーズ（またはシードフレーズ）を実際に保存したことを確認する必要があります。リカバリーフレーズの単語を順番どおりに入力しましょう。
- 5 追加のセキュリティ対策として、一部のウォレットでは安全なパスフレーズを設定できます。なお、秘密鍵と最初のビットコインアドレスは、ウォレットによって自動的に生成されます。

公開鍵はメールアドレスのようなものだと考えてみてください。ビットコインを送ってもらうために、他人と共有する情報です。（例：メールアドレスはメールを送ってもらうために共有します）

一方で、秘密鍵はメールのパスワードのようなものです。これを他人に教えると、その人にあなたのメール（この場合はビットコイン）へのアクセス権を与えてしまうことになるため、共有すべきではありません。

- 6 ビットコインを受け取るには、「受け取り (receive)」アドレスを使用します。自分のウォレットにビットコインを送金しましょう。セルフカストディウォレットでは、法定通貨で直接ビットコインを購入できない場合もあるため、最初に取引所で購入してから送金する必要があるかもしれません。

ビットコインの使い方

クラス演習：選択肢2 - ウォレットを復元する（時間制限あり）



ビットコインウォレットをダウンロードし、生徒ごとに少量のsatsを用意しておきます。
生徒にウォレットを復元するためのシードフレーズが書かれた用紙を配布してください。

以下の手順で、ウォレットの復元を生徒と一緒に進めましょう：

ウォレットを最初に起動すると、ウォレット作成方法が3つ表示されます。

- 1 [Import an existing wallet (既存のウォレットをインポート)]をタップします。
- 2 次に表示される画面で[Restore with recovery phrase (リカバリーフレーズで復元)]をタップしてください。
- 3 12語／18語／24語のリカバリーフレーズを、正しい順番で1語ずつ入力します。
- 4 入力が終わったら[Restore (復元)]をタップします。
- 5 正常にインポートされると「Import Successful (インポート成功)」というメッセージが表示されます。

7.4 受け取りと送金の方法

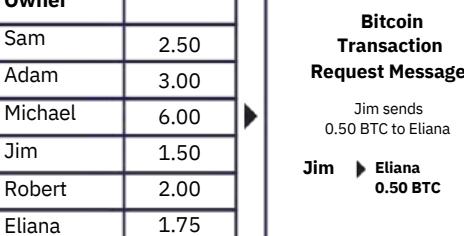
ビットコイントランザクションとは、既存のビットコインの所有権を新しい所有者に移すことです。ただし実際のコインが移動するわけではなく、ネットワーク内のすべてのノードが公開台帳のローカルコピーを更新し、所有権の変更を反映します。

トランザクションを送信する際、送信者は自分の秘密鍵でのみ署名できるメッセージに署名し、ネットワークに対して「このビットコインの所有権が受取人のアドレスに変更された」ことを示します。

こうしてビットコインは新しい所有者だけが送信できるアドレスにひもづけられ、所有権が新しい所有者に移るのです。

LEDGER (台帳)

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniel	5.25

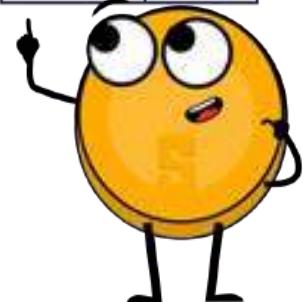


LEDGER (台帳)

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.00
Robert	2.00
Eliana	2.25
Daniel	5.25

新しいビットコイントランザクションは世界中のウォレットから始まるけど、中央の決済処理機関なんて存在しないよ。

その代わりに、世界中のマイナーたちが、トランザクションを台帳に記録するために競い合ってるんだ。



第7章

- ◆ エリアナは自分のアドレスをジムに共有します。
- ◆ ジムは自分のウォレットソフトウェアを使って、トランザクションを作成します。このトランザクションには、エリアナのアドレス、送金額（0.5 BTC）、そしてマイナーへの手数料が含まれます。
- ◆ ジムがトランザクションに署名すると、ネットワークにブロードキャストされ、ノードによって検証されます。ノードはトランザクションが有効かどうかをチェックし、ジムに十分な残高があるかを確認します。不足している場合、そのトランザクションは即座に拒否されます。
- ◆ トランザクションが検証されると、マイナーによってブロックチェーンに追加され、資金はエリアナのアドレスに送金されます。
- ◆ その後、エリアナは自分の秘密鍵を使って、送金された資金にアクセスできます。

一度トランザクションが完了すると、取り消しができない点に注意してください。



ビットコイントランザクションの受け取り方



The screenshot shows a mobile application interface for receiving a payment. At the top, there are 'Back' and 'Done' buttons, and a placeholder text 'Share payment request'. Below this is a large QR code. To the left of the QR code, there is a small amount of text: 'BTC 0.000123456789' and '0.000123456789 BTC'. At the bottom of the screen, there are two buttons: 'Share' and 'Copy'. At the very bottom, there is a link 'Details & Address Settings'.

ビットコインを受け取るには、送信者に自分のビットコインウォレットアドレスを伝える必要があります。

このアドレスは英数字からなる一意（固有）の文字列で、ビットコインネットワーク上でウォレットを識別するために使用されます。

自分のビットコインアドレスは、ウォレットにログインし、「受け取る（Receive）」または「入金する（Deposit）」というオプションを探すことによって確認可能です。

送信者にアドレスを伝える方法はいくつかあります：

- 1 アドレスをコピー&ペースト：アドレスを選択してキーボードで「コピー」を押し、それをメールやメッセージに貼り付けて送信者に伝えます。
- 2 ウォレットへのリンクを共有：一部のビットコインウォレットでは、自分のウォレットへのリンクを作成して送信者と共有できます。リンクをクリックすれば、送信者はそのウォレットにアクセスしてビットコインを送れます。
- 3 QRコードを共有：送信者がスマートフォンでビットコインウォレットアプリを使っている場合、QRコードをスキャンしてアドレスを取得できます。

ビットコインの使い方

送信者があなたのビットコインアドレスを把握したら、そのアドレスと送信したい金額を入力し、送金処理を開始することでビットコインを送ってもらえます。ビットコインはあなたのアドレスに送られ、トランザクションがビットコインネットワークで承認されればウォレットで確認可能です。通常、数分ほどで完了します。

次に、ビットコインの送金方法を見ていきましょう。

ビットコインの送金方法

ビットコインを送るには、ビットコインウォレット・受取人のビットコインアドレス・送信したいビットコインの数量が必要です。

- 1 ビットコインウォレットを開きます。電話番号にSMSコードが送信されるので、ダイアログボックスに入力します。
もしくは、Googleの2段階認証を有効にしている場合は、Google Authenticatorアプリの6桁コードを入力します。
※翻訳者注釈：このような手順は、カストディ型ウォレットに見られる特徴です。
- 2 受取人のアドレスを取得し、「送金 (Send)」または「出金 (Withdraw)」機能に移動します。
- 3 コピーしたアドレスを「宛先 (To)」欄に貼り付けます。
- 4 「金額 (Amount)」欄に送金したいビットコインの数量を入力します。
- 5 受取人のアドレスと送金額を再確認します。
- 6 「確認して送金 (Confirm and Send)」をクリックする前に、トランザクションの詳細を再確認し、正しいアドレスに正しい金額が送られることを確認してください。
- 7 トランザクションを確定し、ネットワークによるトランザクションの承認を待ちます。

これで、自分で管理するビットコインウォレットの評価・選択・設定方法への理解が深まりました。ビットコインネットワーク上で、あるウォレットから別のウォレットへビットコインを送金することは「オンチェーン」取引と呼ばれます。これは、トランザクションがビットコインのメインネットワーク（ブロックチェーン）上で行われるからです。オンチェーン取引はビットコインを取引する最も安全な方法です。ただし、オンチェーン取引は、第8章で解説するライトニング取引などの他のオプションよりも遅く、費用も高くなることがあります。

アクティビティ：ビットコイン送受信の実践

目的：ピア・ツー・ピアで行われるビットコイントランザクションの仕組みと基本的な概念を理解する

始める前に、ビットコイントランザクションにおける主要なプレイヤーについて、簡単にさらいましょう：

- 送信者と受信者：相互に取引を行う当事者。
- ノード：トランザクションを検証し、ブロックチェーンの完全なコピーを保存します。
- ライトノードは、ブロックチェーンの全データを保存するフルノードに比べて、少ないストレージと計算リソースでトランザクションを確認できます。
- マイナー：新しいトランザクションをブロックチェーンに追加する役割を担います。

第7章

アクティビティにおける自分の役割を理解しましょう。あなたには、送信者、受信者、ノード、マイナーのいずれかの役割が割り当てられます。

- ◆ 送信者：トランザクションの作成とブロードキャストを担当します。
- ◆ 受信者：トランザクションの受け取りと検証を担当します。
- ◆ ノード：トランザクションの検証を担当します。
- ◆ マイナー：トランザクションをブロックチェーンに追加する役割を担います。

トランザクションの検証は、受信者とノードの両方が行う必要があります。

◆ **送信者：**トランザクションを作成します。

以下の手順に従ってください：トランザクション用のメモ用紙に、送信したいコインの数と受信者の名前またはイニシャルを記入します。
次に、自分の名前またはイニシャルで署名を行い、秘密鍵のシミュレーションとします。
その後、トランザクションメモと対応する数のコインを受信者に渡します。

◆ **受信者：**トランザクションの検証を担当します。

- ◆ トランザクションメモを確認し、コインの枚数と受信者の名前またはイニシャルが正しく書かれているかチェックします。
- ◆ 受け取ったコインを数えて、メモに書かれたコインの数と一致するか確認します。
- ◆ コインが一致したら承認欄にチェックを入れます。一致しない、または疑問がある場合は、そのトランザクションを拒否します。

コイン送信記録	送信者	送信者署名	受信者	日付と時刻	受取人の承認

◆ **ノード：**トランザクションを検証します。

あなたはトランザクションが有効かどうかを確認する責任があります。

- ◆ 送信者と受信者の名前（またはイニシャル）が有効であることを確認してください。
- ◆ 送信者に十分な残高があるか、またそのトランザクションがコインの二重支払いをしていないかを確認してください。

コイン送信記録	送信者	送信者署名	受信者	日付と時刻	ノードの承認

ビットコインの使い方

④ **マイナー：** トランザクションをブロックチェーンに追加する役割を担います。以下の手順に従ってください。

- ⚙️ 受信者が確認し、ノードが検証したトランザクションをチェックします。
- ⚙️ サイコロを振って、他のマイナーと数字を比べます。より小さい数字を出したマイナーが、そのトランザクションをブロックチェーンに追加します。
- ⚙️ サイコロで勝ち、トランザクションを追加できたマイナーには、時間と労力への報酬として1ポイントが与えられます。アクティビティ終了時に最も多くのポイントを獲得したマイナーが勝者です。

**一度ブロックチェーンに追加されたトランザクションは、変更も取り消しもできません。

⑤ **コイン残高を追跡する：** アクティビティの間は、自分のデジタルウォレットにあるコインを数えて、コイン残高を記録し続けましょう。

コイン送信記録	送信者	送信者署名	受信者	日付と時刻	追加の承認

⑥ アクティビティで学んだ概念について、クラスで話し合いましょう。

7.5 ビットコインで貯蓄する

ビットコインは正しく使えば、インフレから資産を守り、他者から支配されることを防ぐ力を持っています。
ビットコインによる貯蓄は、資産を蓄積し、長期的に富を築くための有効な方法です。

ここまで学んできたように、どんなお金で貯蓄するかという選択は、非常に重要な決断の1つです。
賢く選ぶことで、自分自身や家族にとってより良い将来につながります。



安心感： 適切に保管すれば、ビットコインは誰にも奪われる
ことのない唯一の財産形態になります。



第7章

7.6 *Don't Trust, Verify - 信じるな、検証せよ*

ビットコインで何をするにしても、これだけは覚えておいてください：
「*Don't Trust, Verify*（信じるな、検証せよ）」。

ビットコインにはリーダーが存在しません。
誰かの主張を盲目的に信じてはいけません。
常に疑問を持ち、自分自身で検証すべきです。

この信条に従うことで、ビットコインを失うリスクから身を守れます。
「次のビットコインはこれ！」「投資のチャンス！」「簡単に儲かる！」といった主張に流されず、
自分の資産をしっかり守れるようになります。

第7章では、日常生活でビットコインを使うための重要なスキルを身につけました。
ビットコイン入手・交換するさまざまな方法や、ウォレットを使って安全に保管する方法を学びました。

モバイルビットコインウォレットを設定し、他の人と実際に取引を行うことで、ビットコインを日常的に、
自信を持って使うための実践的な経験を得ました。
お金貯める方法としてビットコインを理解し、「信じるな、検証せよ」の考え方へ従うことで、
自分自身でお金を管理できるようになったのです。

次の章では、ライトニングネットワーク（Lightning Network）について学びます。
この革新的な技術が、世界中の人々の「お金へのアクセスと使い方」をどのように変えているのかを見ていきましょう。
日常的な取引から、より高度な応用まで、ライトニングネットワークが個人・コミュニティ・ビジネスに対して、
どのように金融サービスへのアクセスを提供しているのかを探ります。

第8章： ライトニングネットワーク —日常生活でビットコインを使う

8.0 はじめに

アクティビティ：「ビットコイン ライトニングネットワーク解説動画・
実際の仕組み」を視聴

8.1 ライトニングネットワーク

8.2 ライトニングウォレットの種類

- 8.2.1 セルフカストディウォレットvsカストディ型ウォレット
- 8.2.2 オープンソースvsクローズドソース

8.3 ビットコイン・ライトニングウォレットの設定

8.4 ライトニングでの送受信

アクティビティ：ライトニングウォレット・リレーレース

8.5 ビットコインでコーヒーや食料品を買う

- 8.5.1 オンライン：ECサイトでの決済プラグイン
- 8.5.2 対面：地域の対応店舗を探す
- 8.5.3 一時的なツール：ギフトカード・決済に使えるカード
- 8.5.4 循環型経済と交換手段としてのビットコイン

生徒用ワークブック

日本語版 | 2025年版

ライトニングネットワーク： 日常生活でビットコインを使う

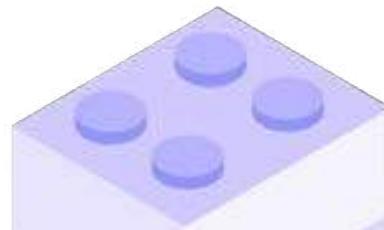
8.0 はじめに

「私たちはビットコインのためのVisaネットワークを構築している。
しかし、私が素晴らしいと思うのは、Visaとは違い、誰でもその上に構築できることだ。」

エリザベス・スターク

テクノロジーは通常、層（レイヤー）のように積み重なる形で成長・拡張していきます。
お気に入りのウェブサイト、メール、ソーシャルメディアを考えてみてください。それらはインターネットプロトコルの上に構築され、インターネットはコンピューターの上に、
コンピューターは電気の上に、といった形で成り立っています。
こうした技術は、非常にシンプルな設計から始まり、時間をかけて改良されてきました。

ビットコインも例外ではありません。
「ビットコインはお金のインターネットである」——これは、
アンドレアス・アントノプロスの有名な言葉です。
ビットコインは健全なデジタルマネーの基礎レイヤーであり、
その上に新しいテクノロジーが構築される堅固な土台を提供します。

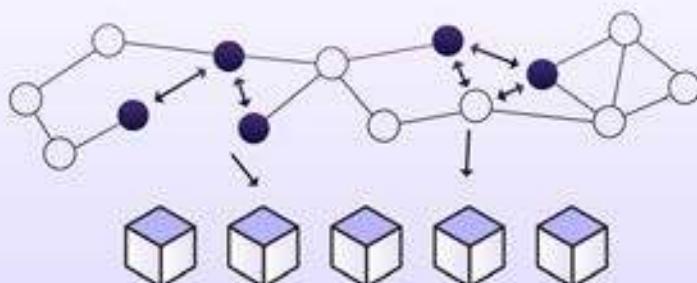


APPLICATION

ソフトウェアバックエンド

コネクティビティ（接続性）

ハードウェア



これらの層の1つが「ライトニングネットワーク（Lightning Network）」と呼ばれています。

これはビットコインのための超高速道路のようなもので、人々がビットコインを素早く、かつ非常に低い手数料で送受信できるようにします。

ライトニングネットワークは通常のビットコインネットワークの上に、小額で即時取引できる仕組みを実現しました。これにより、コーヒーを買ったり、友人にお金を送ったりといった行為が、シンプルかつ高速になるのです。

おさらい：サトシ（satoshi）とは、ビットコインの最小単位のことです。

ドルがセントに分けられるように、1ビットコインも「サトシ」と呼ばれる小さな単位に分割できます。1ビットコインは1億サトシに相当し、サトシはビットコインシステムにおける最小の価値単位です。

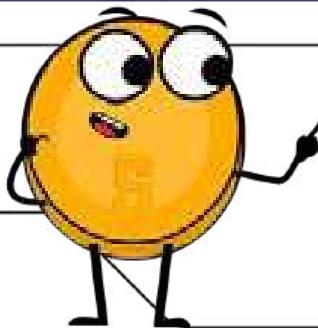
この章では、ライトニングネットワークでビットコインを送る話をする時、「satsを送る（sending sats）」という表現を使います。つまり、ビットコインの小さい単位を送るということです。

Sats	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

第8章

アクティビティ：

「ビットコイン ライトニングネットワーク解説動画：
実際の仕組み」を見てみよう



8.1 ライトニングネットワーク

先ほど見たように、ライトニングネットワークは決済システムとして機能し、ビットコインによる素早く低コストな取引を可能にします。

これは、両当事者がいくらかのビットコインを入金した共有ウォレットを確立することで動作します。その中で複数回の取引を行っても、1つ1つの取引をメインの台帳（ブロックチェーン）に記録する必要はありません。すべての取引が終わった後、最終的な残高だけがブロックチェーンに記録されます。



ライトニングネットワークは、ビットコインを使って迅速かつ安価に送受信できるようにする決済システムです。

この仕組みでは、両者がビットコインを入れた共有ウォレットを設定し、メインのブロックチェーンに記録することなく、互いに無制限の取引を行うことができます。

そしてすべての取引が終了すると、最終的な残高だけがメインのブロックチェーンに記録されるのです。

カフェで一日仕事をする場面を想像してみてください。一日中滞在する予定なので、その都度支払うのではなく、最初に一定額を前払いしてお店に預けておきます。

一日の終わりに帰る準備ができたら、お店の人と一緒にその記録を確認して、最終的な会計を済ませます。もし前払いした金額が実際に使った額より多ければ、使わなかった分は返金されます。

次に、数千人が同時に同じような仕組みを使い、さらに他の人がその仕組みを通じて別の人とつながることをイメージしてみてください。

それがライトニングネットワークです！

ライトニングを使えば、直接チャネル※を開いている相手だけでなく、ネットワーク上の誰にでも支払いを送ることができます。

※チャネル...ふたりの間であらかじめ開いておく送金専用の通路

たとえ受取人と直接つながっていなくても、

支払いはネットワーク上の経路を通って目的地へと届けられるのです。

第7章で扱ったオンチェーン取引と、ライトニングネットワークのようなオフチェーン取引の違いを見てみましょう。

オンチェーン取引：

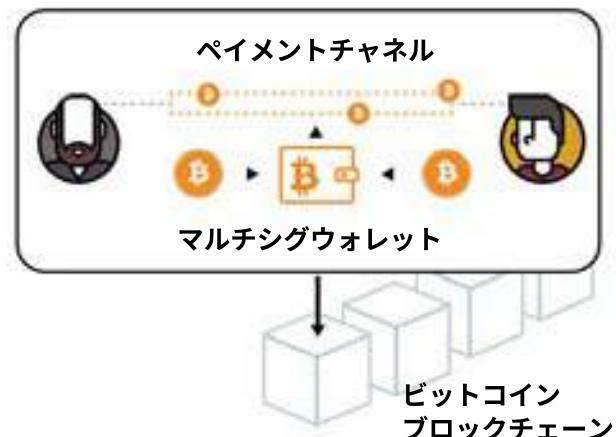
- ・ビットコインのブロックチェーン上で直接行われる取引です。
- ・承認にはおよそ10分かかります。
- ・手数料はトランザクションのバイトサイズによって異なります。
- ・より安全ですが、速度は遅めです。



ライトニングネットワーク： 日常生活でビットコインを使う

オフチェーン取引（ライトニングネットワーク）：

- ・ビットコインブロックチェーンの上に構築された、別のネットワーク上で行われる取引です。
- ・より速く、低い手数料で決済が行われます。
- ・規制や法律が採用を後押しする環境や、取引のスピードやコストが重視される場面でよく利用されます。
- ・オンチェーン取引と比較すると、セキュリティは低くなります。



支払い ネットワーク	ビットコインネットワーク	ライトニングネットワーク
定義	暗号技術を使って金融取引を保護する、分散型のデジタルネットワーク。	ビットコインブロックチェーン上に構築された第2層の決済プロトコルで、より高速かつ安価な取引を可能にする。
利点	分散型で安全。チャージバック（支払い後の勝手な取り消し）や詐欺の心配がない。匿名で利用可能。グローバルに受け入れられている。	より高速で低コストな取引ができる。スケーラビリティ（拡張性）の向上。オフチェーン取引はブロックチェーンを詰まらせない（混雑を招かない）
欠点	取引に時間がかかる。 取引の種類によっては手数料が高い。 初心者には仕組みが複雑。	チャネル運営者への信頼が必要。 まだ実験段階で広く普及していない。 チャネルの開閉にはオンチェーン取引が必要。

第8章

8.2 ライトニングウォレットの種類

ライトニングウォレットはビットコインウォレットとは少し異なりますが、基本的な役割は同じで、ビットコインの受け取りと送信ができます。

違いは、ライトニングウォレットでは、ビットコインネットワークの上に構築された第2層であるライトニングネットワークを使って送金する点です。

前の章で紹介したビットコインウォレットと同様に、ライトニングウォレットを選ぶ際も考慮すべきさまざまな特徴があります。

8.2.1 セルフカストディ型ウォレット vs カストディ型ウォレット

ビットコインウォレットと同様に、セルフカストディ型のライトニングウォレットでは自分で秘密鍵を管理します。一方、カストディ型では他の人が秘密鍵を管理します。

カストディ型ウォレットを使う場合、自分のウォレットへのアクセスはできますが、実際にお金を使うためには第三者の許可が必要です。つまり、利便性のために資産の所有権を手放しているのです。

少額であればカストディ型でも許容できる場合がありますが、技術を理解したらセルフカストディウォレットの使用が推奨されます。

ここから先は、セルフカストディ型のライトニングウォレットのみに焦点をあてて説明していきます。

8.2.2 オープンソース vs クローズドソース

前の章で紹介したビットコインウォレットと同じように、ライトニングウォレットもオープンソースとクローズドソースに分類されます。

常にオープンソースのウォレットを使うようにしましょう。これらは検証できるように完全に公開されており、コミュニティによってチェックされているからです。

オープンソースのアプリケーションであれば、誰でもソフトウェアの改良に貢献できるため、ユーザーにとってもよりよい選択肢になります。

8.3 ビットコイン・ライトニングウォレットの設定

セルフカストディ型のビットコイン・ライトニングウォレットを設定する方法は、オンチェーンのセルフカストディ型ビットコインウォレットと同じです。

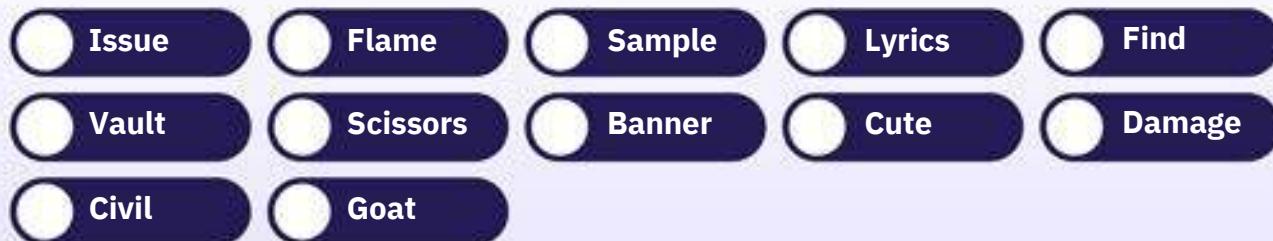
ライトニングネットワーク： 日常生活でビットコインを使う

クラス演習 – オプション1：新しいセルフカストディ型ライトニングウォレットをダウンロードする

ビットコイン・ライトニングウォレットの作成と使い方

- 1** App Store (iOS) またはGoogle Playストア (Android) でアプリを検索します。
- 2** アプリを開き、12語または24語のリカバリーフレーズ（シードフレーズとも呼ばれます）を入力します。必ず紙に書き留め、安全な場所に保管してください。このリカバリーフレーズがあれば、万が一のときに資金へのアクセスを復元できます。
- 3** この単語の並びを失くしたり忘れたりすると、ウォレットへのアクセスを失ったときにビットコインにアクセスできなくなるのでご注意ください。
- 4** リカバリーフレーズを本当に保存したかどうかを確認するために、それらの単語を同じ順番で入力する必要があります。
- 5** 追加のセキュリティ対策として、安全なパスフレーズを設定できるウォレットもあります。なお、秘密鍵と最初のビットコインアドレスは、ウォレットによって自動的に作成されます。
- 6** ビットコインを受け取るには、ライトニングインボイス（請求書）、アドレス、またはQRコードを生成します。そしてウォレットにビットコインを転送してください。セルフカストディウォレットでは、法定通貨で直接ビットコインを購入できない場合があるため、取引所で購入してから転送する必要があるかもしれません。

あなたのシードフレーズ（例） シードフレーズは、アカウントの生成と復元に使われます。



これらの12単語を紙に書いて保管してください。順番がとても重要です。
シードフレーズがあれば、あなたの資産へのアクセスを復元できます。

※カストディ型ウォレットを使う場合、セクション8.3のいくつかの手順は行いません。
カストディ型ウォレットにはリスクが伴います。秘密鍵を自分で管理しないため、自分の資金の管理権限も持たないことになるからです。

ウォレットの設定が完了したので、次はライトニング取引の受け取りと送信、および第7章で行ったオンチェーン取引との違いを見ていきましょう。

第8章

8.4 ライトニングでの送受信

ライトニングウォレットを使うと、ビットコインの利用は高速・低成本かつプライバシーが保護され、個人間の取引が簡単になります。

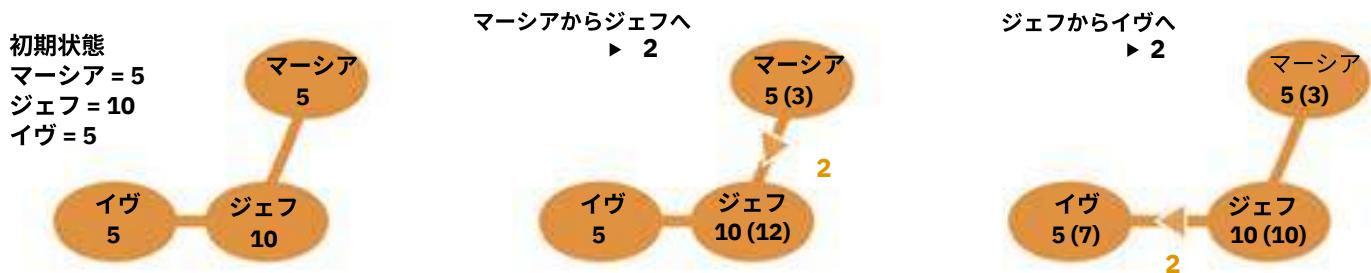
コーヒーを買ったり買い物をしたりといった日常の支払いに、素早くビットコインを送受信できます。ここでは、ライトニングネットワークが実際にどのように動くのか、いくつかの例で見てみましょう。

例1：

以下の例では、マーシアとイヴがそれぞれ「5」のお金を持っています。

マーシアはそのうち「2」をイヴに送りたいと考え、まず「2」をジェフに渡します。
ジェフはその「2」をイヴに渡し、イヴは「7」に増えました。マーシアは「3」になりました。
これで取引は完了です。

重要な点は、マーシアとイヴが銀行などの仲介機関を通さずに取引できることです。



この場面では、マーシアとイヴが直接信頼し合っていないため、ジェフが仲介者、つまり「信頼された第三者」として機能します。

マーシアから「2」を受け取ったジェフは、それをイヴに渡すことで取引を完了させます。ジェフを仲介者として利用することで、マーシアとイヴは銀行や中央集権的な機関を介さずに取引を実行でき、より速く・安く・安全なやり取りが可能になるのです。

ジェフはこのピア・ツー・ピア取引プロセスにおいて重要な存在です。

ライトニングネットワークのノードオペレーターとして、ジェフには以下のようなメリットがあります：

1 取引手数料

ジェフは、自分のノードを経由する各トランザクション（取引）から少額の手数料を受け取ります。これはノードの維持や運営にかかる時間と労力に対する報酬となります。

2 ネットワークへの参加

ライトニングノードを運営することで、ジェフはネットワークの分散性・セキュリティ・安定性の向上に貢献しています。これにより、信頼できるノードオペレーターとしての評価や信頼性が高まり、将来の取引においてより魅力的な仲介者となる可能性があります。

ライトニングネットワーク： 日常生活でビットコインを使う

3

ネットワークの成長

ライトニングネットワークの利用者が増えるにつれて、ジェフのノードを通過するトランザクションの数も増加する可能性があり、取引手数料から得られる収益も増えるかもしれません。

4

ネットワークセキュリティの向上

ジェフは仲介者として、マーシアとイヴの間にもう1つの保護層を加えることで、ネットワーク全体のセキュリティ向上に貢献します。これによりユーザーのネットワークへの信頼も高まり、新たな利用者の参加を促進し、ネットワークの成長につながる可能性があります。

このように、ライトニングネットワークのノードオペレーターになることは、ジェフにとって収入を得られるだけでなく、ネットワークの発展や成長に貢献できる機会にもなるのです。

まとめると、オンチェーン取引は時間がかかる代わりにより安全で、オフチェーン（ライトニングネットワーク）取引は高速ですがセキュリティはやや劣ります。自分のニーズに応じて、セキュリティと速度のトレードオフを考えて選びましょう。

例2：

ミーナはマクドナルドが大好きで、毎日朝・昼・晩すべてそこで食べています！

ですが、支払い方法がいろいろあり、どれが一番いいのか悩んでいます。

ビットコインとライトニングネットワークについて少し学んでいたミーナは、下の表を比較した結果、ライトニング決済が最良の選択だと考えました。

ライトニングネットワーク vs 従来の銀行システム

利点	ライトニング ネットワーク	従来の 銀行システム	利点	ライトニング ネットワーク	従来の 銀行システム
スピード	速い	遅い	スケーラビリティ	高い	低い
透明性	透明	不透明	プライバシー	高い	中程度
セキュリティ	安全	脆弱	相互運用性	高い	低い
取引手数料	低い	高い	法令遵守	中程度	高い
金融包摂	高い	限定的	費用対効果	高い	中程度

Visa, Inc.

平均して毎秒
1,700件の取引を
処理。



最大処理能力は
毎秒65,000件。

ビットコインオンチェーン



毎秒7件の
取引処理能力

ビットコイン
ライトニングネットワーク



毎秒数百万件の
取引が可能。

第8章

ミーナは、スピードで安全かつコスト効率のよい取引を好むため、マクドナルドでの支払いにライトニングネットワークを使うことにしました。ライトニングを使えば、支払いが瞬時に、安全に、しかも低い手数料で処理されるので、食事をより楽しめます。

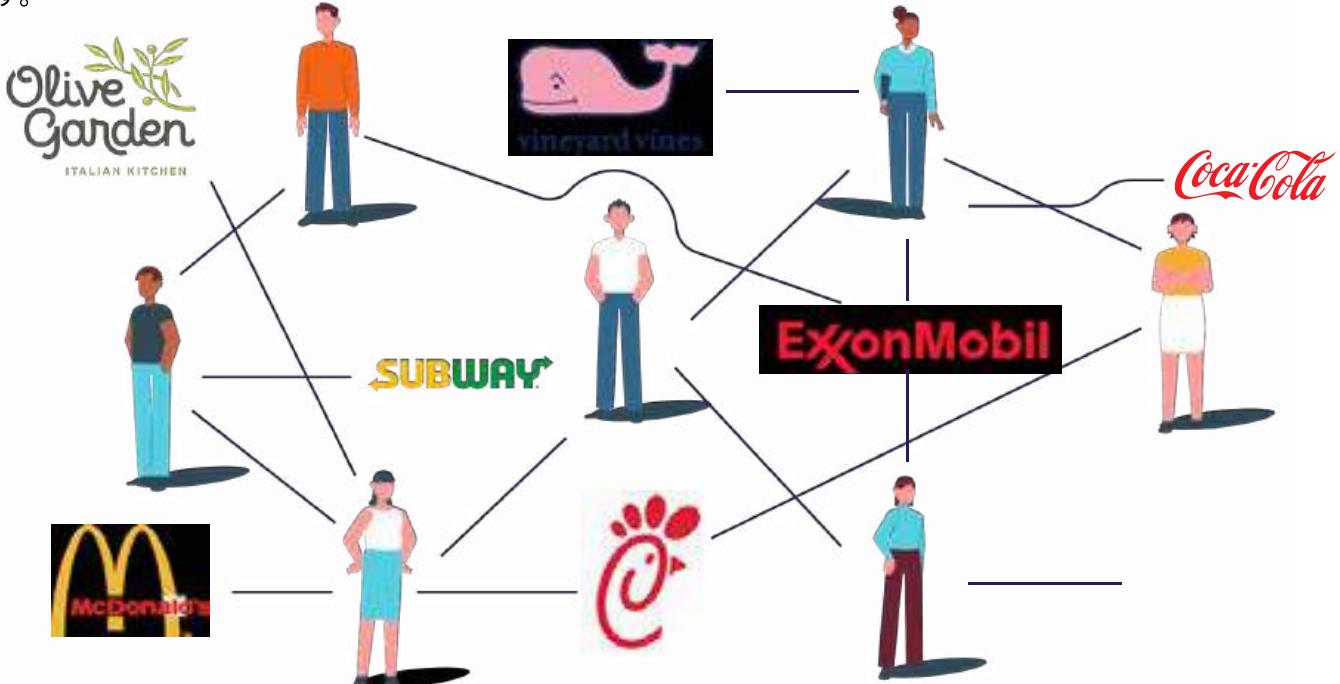
さらに、ライトニングネットワークは金融包摂を可能にするため、ミーナはエルサルバドルの都市部から離れた場所にいても、食事代を支払えるのです。

※金融包摂...すべての人が経済活動に必要な金融サービスを利用できる状態

ライトニングネットワークの利用を始めるために、まずミーナはスマホにライトニングウォレットをダウンロードします。そして、通常のビットコインウォレットから新しいライトニングウォレットにビットコインを送金して、ウォレットに資金を補充します。

なお、セルフカストディウォレットの場合、チャネルの開設（特定の相手との双方向の支払い経路を開くこと）が必要になることがあります。

ミーナは自分が無理なく利用できる任意の金額のビットコインを補充できますが、ライトニングネットワークのチャネルにロックされたビットコインは、チャネルを閉じるまではオンチェーン取引には使えない点に注意が必要です。



ライトニングウォレットに資金を補充したら、ミーナはそれを使ってマクドナルドで支払いができるようになります。マクドナルドがライトニングネットワークに参加していれば、ミーナはマクドナルドと直接チャネルを開くか、既存のチャネル経由で支払うことができます。

この時、ビットコインはビットコインのブロックチェーンから、ライトニングネットワーク上のオフチェーン取引へと移されます。

支払いチャネルがすでに開かれていれば、ミーナは新しいチャネルを開いたり、毎回高額な手数料を払ったりすることなく、マクドナルドでスムーズな買い物ができます。
チャネルが維持されていれば、ミーナは何度でも手軽に支払い可能です。

例えば、ミーナが0.0005BTCでハンバーガーを買うと、チャネルはミーナの残高が0.9995BTCになったことを記録します。そして翌日0.0003BTCでミルクシェイクを買うと、チャネルは残高が0.9992BTCになったことを記録します。

ライトニングネットワーク： 日常生活でビットコインを使う

ミーナがマクドナルドと直接チャネルを開設している場合、ビットコイン残高を別の目的に使いたいと思った時は、チャネルを閉じるためのトランザクションをビットコインのブロックチェーンにブロードキャストして、チャネルを閉じます。

これは、ライトニングウォレット内でチャネルを閉じるトランザクションを開始することで行われ、そのトランザクションには、両当事者が合意した最終的なチャネルの残高が含まれています。その後、トランザクションはビットコインのブロックチェーンにブロードキャストされ、マイナーによって承認されます。

トランザクションが承認されると、チャネルは閉じられ、チャネルに残っていたビットコインはミーナとマクドナルドに返還されます。

チャネルを閉じるトランザクションがブロックチェーン上で承認されるまでには、時間がかかることがある点に注意が必要です。

この待機期間中、資金はチャネル内にロックされたままで、オンチェーン取引には使えません。

トランザクションが承認されると、ミーナには通知が届きます。

ライトニングウォレットの設定と、ライトニングネットワークを使った送金方法について学んできました。次は、クラスの他の生徒にsats（ビットコインの最小単位）を送るゲームをプレイしてみましょう。



これは世界全体の地図です。

ライトニングネットワークを使えば、ビットコインのライトニングウォレットを持つユーザーに誰でもsatsを送ることができます。

支払いは数秒で届き、手数料はほとんどかかりません。

さあ、自分で試してみましょう！



第8章

アクティビティ：ライトニングウォレット・リレーレース

- 1** まず、ライトニングウォレットをスマートフォンやパソコンにダウンロードする必要があります。
- 2** この章のセクション8.3にある手順に従って、ウォレットをインストールしてください。
- 3** ウォレットのインストールが完了したら、それを開いて指示に従いセットアップしてください。
新しいウォレットを作成するか、既存のウォレットを復元します。パスワードや他の認証手段で保護する作業が必要になるかもしれません。
- 4** ビットコインを受け取るために、ライトニングインボイス・アドレス・QRコードのいずれかを生成してください。
- 5** ウォレットの準備が整い、satsを受け取れる状態になったら、先生があなたとあなたのグループに対して、開始用のsatsを直接ウォレットに送ってくれます。



- A** グループの目標は、ライトニングネットワークを使って、satsを最初の人から次の人へと順番に送っていき、最後の人まで届けることです。
- B** 他の人にsatsを送るには、ウォレットを開いて送金手順に従ってください。受取人のライトニングインボイスを入力するか、QRコードをスキャンし、送金したいsatsの量を入力します。
- C** 一番早く、satsを最後の人に送るのに成功したグループが勝者です！（そしてそのsatsはキープできます）

この活動を通じて、グループで大変だったことを話し合ってください。
送金は簡単で、スピーディーで、手数料は安かったでしょうか？
ライトニングネットワークは使いやすく、理解しやすいと思いましたか？

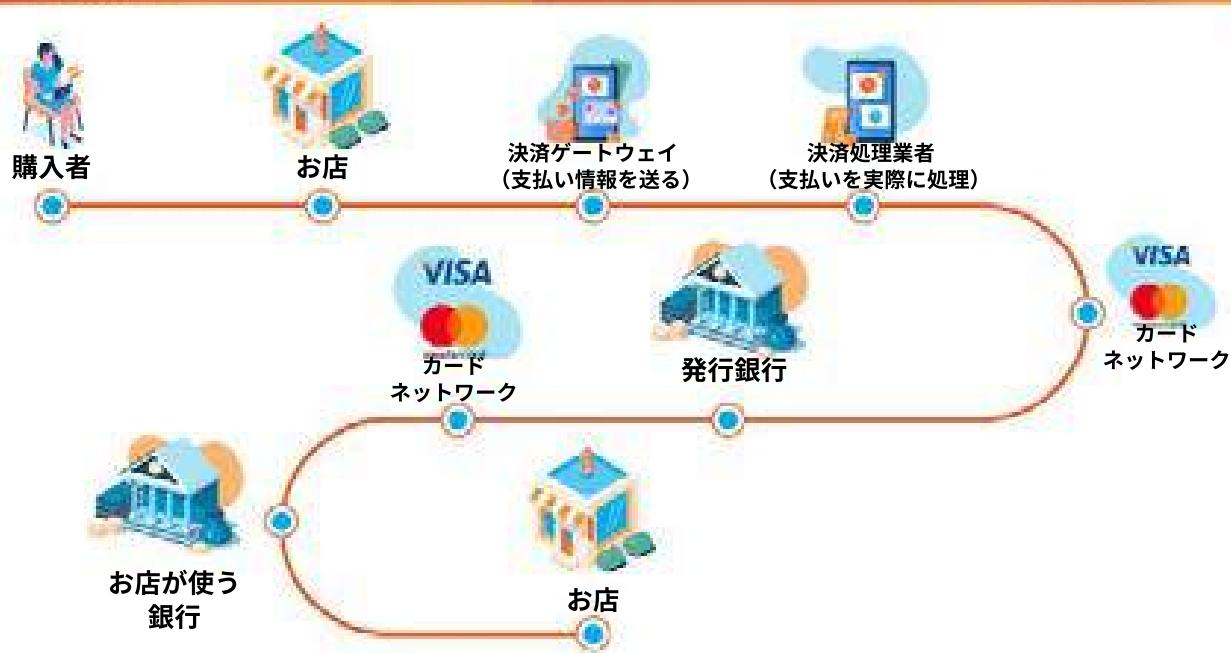
ライトニングネットワーク： 日常生活でビットコインを使う

8.5 ビットコインでコーヒーや食料品を買う

毎日のコーヒーや食料品の買い物にビットコインが使えたらしいのに、と思ったことはありませんか？ 実は、使えるんです。オンラインでも実店舗でも、ビットコインで支払える選択肢は数多くあります。ここでは、ビットコインが使えるお店を見つけるのに役立つ方法やツールをいくつか紹介します。

クレジットカードやアプリでの支払いは、支払う側にとっては簡単に見えるかもしれません。しかし実際には多くの関係者が関わり、かなり複雑な処理が行われています。

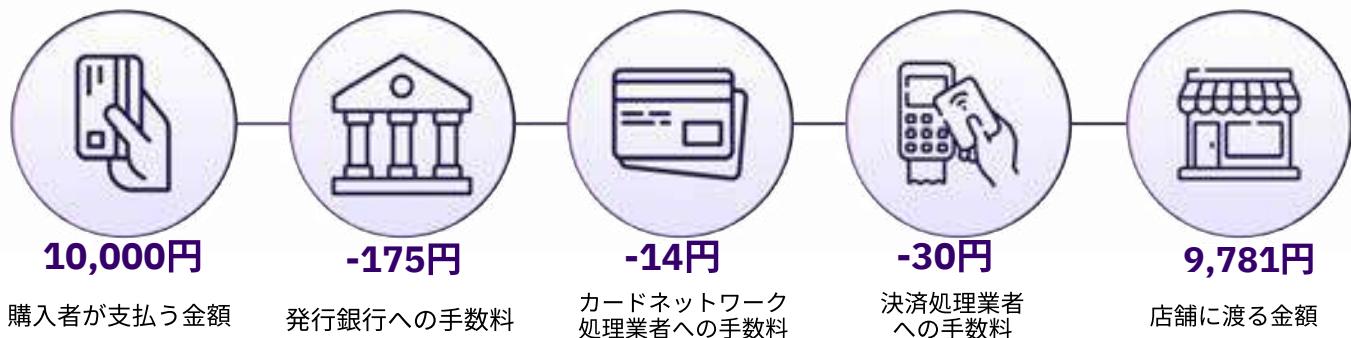
支払い処理の仕組み



買い物をする時には、多くの関係者が関わっており、それぞれが手数料を取ります。店舗のオーナーにとって、これらの手数料は高額になることがあります。価格の3%以上になることもあります。これは彼らにとって大きな負担です。そのうえ、為替手数料が発生することもあります。

第8章

クレジットカードの決済手数料（例）



ビットコインとライトニングネットワークを使えば、企業は世界中から、オープンで安全かつ、インターネットを前提に設計された、国境も検閲もないお金の仕組みを通じて、即時に支払いを受け取れます。

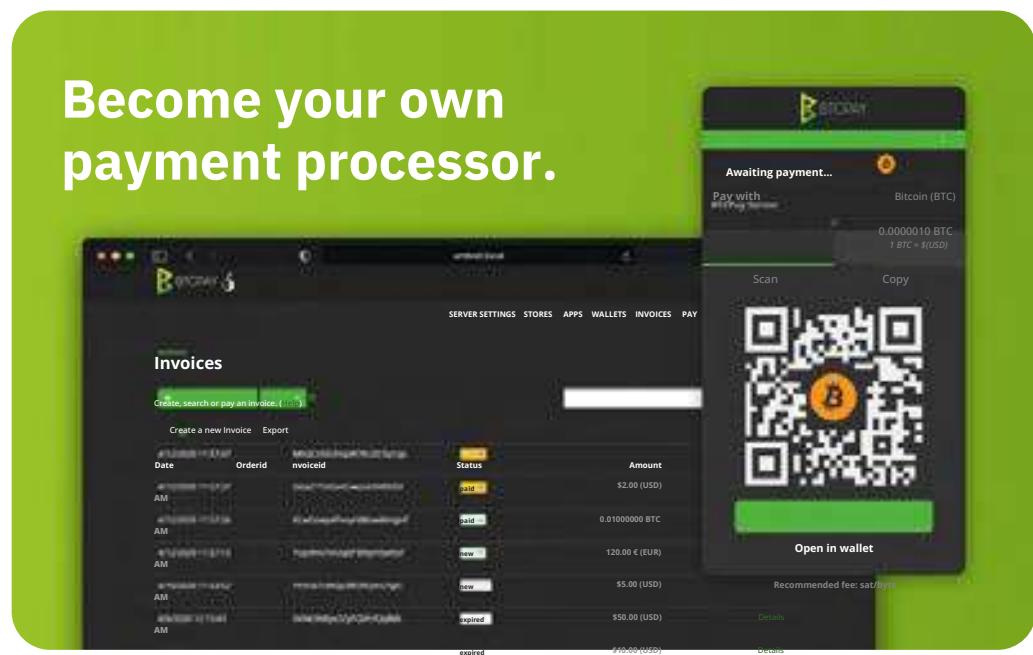
次に、店舗がビットコイン支払いを簡単に導入する方法をいくつか紹介します。

8.5.1 オンライン：ECサイトでの決済プラグイン

BTCPay Serverはオープンソースの決済処理ツールで、店舗はわずかな技術的な知識のみでもビットコイン支払いを受け入れられます。

完全に無料で、手数料も一切かかりません。

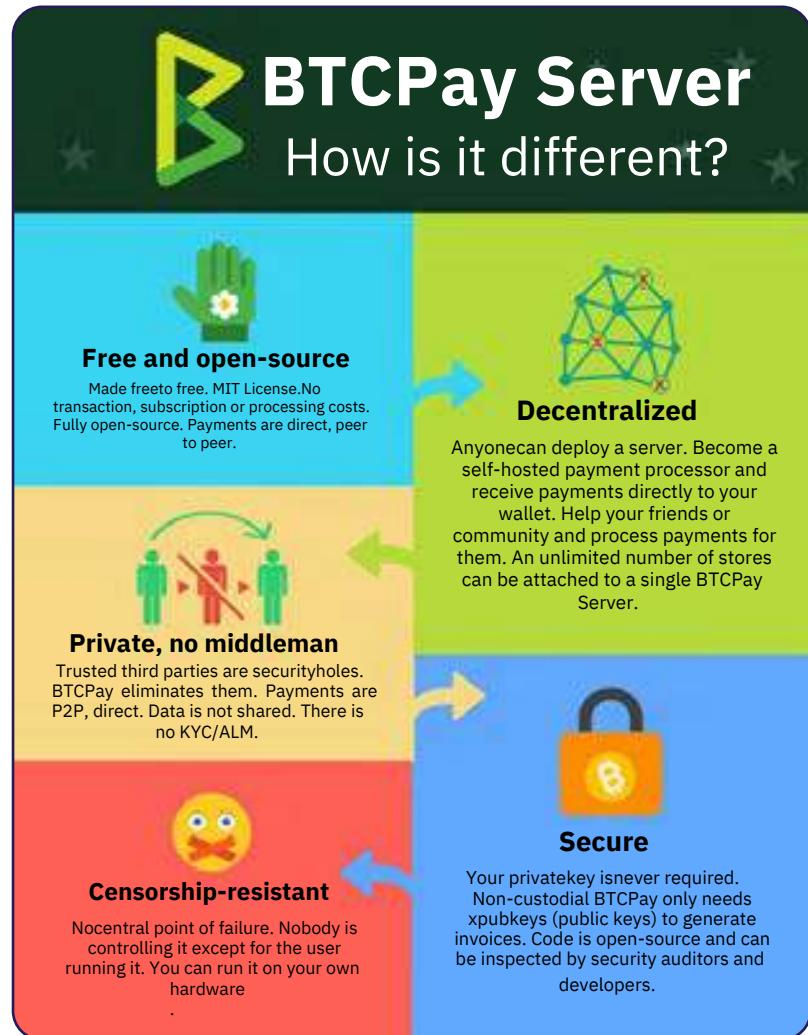
オンラインの店舗は、自分のウェブサイトにBTCPayプラグインを追加するだけで、BTCPay Serverをスムーズに導入できます。



ライトニングネットワーク： 日常生活でビットコインを使う

BTCPay Serverは企業ではなく、
オープンソースのプロジェクトです。
仕組みやコンピュータープログラミングに
ついて理解が深まれば、誰でもこの
プロジェクトに貢献することができます。

BTCPayServerの詳細や、
対面またはオンラインビジネスでこの決済
システムを使う方法については、
以下の公式サイトをご覧ください。
<https://btcpayserver.org/>



8.5.2 対面：地域の対応店舗を 探す



実店舗でもBTCPay Serverを使い、
ビットコイン支払いを受け入れることができます。
または、ビットコインウォレットを
スマートフォンにダウンロードして、
ビットコインによる支払いを直接受け取ることも可能です。



第8章



ビットコインを受け入れている近くのお店を探すには、BTCMap.orgにアクセスして、自分の地域を検索します。 BTCMap.orgは、ビットコイン決済対応店舗が情報を登録できる、オープンソースの地図です。 ビットコインを使いたい人にとって非常に便利なツールです。

BTCMap.org
Easily find places to spend sats anywhere on the planet.

The screenshot shows the BTCMap.org mobile application interface. On the left, there's a navigation bar with icons for globe, camera, Android, play store, and a person. The main area is a map of Los Angeles, California, with several green location pins placed across the city. Labels for neighborhoods like Universal City, Glendale, Atwater Village, Elysian Valley, Echo Park, West Hollywood, Beverly Hills, Beverlywood, Adams-Normandie, Leimert Park, Al-Alameda, Chesterfield Square, Inglewood, Huntington Park, and South Gate are visible. Each pin indicates a location where Bitcoin is accepted.

8.5.3 一時的なツール：ギフトカード・決済に使えるカード

まだビットコインを受け入れていない店舗の商品やサービスをビットコインで購入したい場合は、仲介手段として「ギフトカード」を使う方法があります。

一部の事業者は、ビットコインと引き換えにギフトカードを売買するサービスを提供しています。行きたいお店が対応しているギフトカードをビットコインで手に入れれば、そのカードを店舗で利用可能です。

国によっては、飛行機のチケット・ホテル・ゲーム・SIMカードなど、ビットコインとギフトカードがあれば、ほとんど何でも購入できます。

8.5.4 循環型経済と交換手段としてのビットコイン

循環型経済という概念は、できる限り多くの製品や副産物を再利用し、リサイクルすることで、経済活動における廃棄物を最小限に抑えようとする考え方由来します。

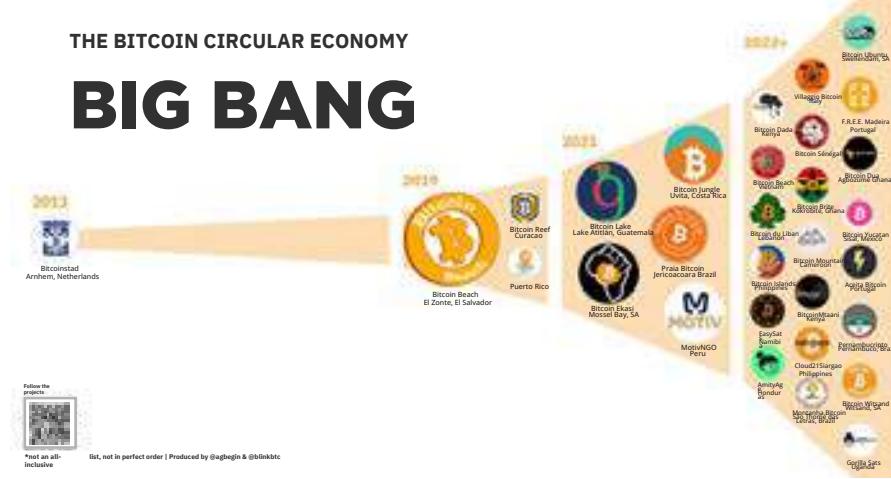
この考えに基づいた「ビットコイン循環経済」では、取引がビットコインで行われ、経済の中でビットコインが循環・蓄積・導入拡大していくことで、個人や事業者に利益をもたらします。



ライトニングネットワーク： 日常生活でビットコインを使う

ライトニングネットワークによって、ほぼ即時かつ低手数料のビットコイン取引が可能となり、ビットコイン循環経済の世界中での発展を可能にしています。

世界で最初に誕生したビットコイン循環経済は、オランダのアーネムにあります。これはライトニングネットワークが登場するよりもずっと前に作られたのですが、当時はオンチェーンの手数料が非常に低かったのです。



2番目に生まれたのは、エルサルバドルのエル・ソンテにある Bitcoin Beach (ビットコイン・ビーチ) です。ライティングネットワークの力を活用し、銀行口座を持たない人が多い地域社会の中で、スマートフォンを使った即時のデジタル決済ができるようになりました。

現在では、ビットコイン、ライトニングネットワーク、そして教育的な取り組みによって、世界中で何百ものビットコイン循環経済が生まれています。



第8章

BTCTMap.orgでは、他のビットコインユーザーと出会えるビットコインコミュニティや、ビットコインを受け付ける事業者を探すこともできます。私たちの教師や生徒の中には、実際にお店や循環経済の情報をBTCTMap.orgに追加した人もいます。あなたも準備ができたら、ぜひやってみてください！



 **BTCTMap.org**

Easily find places to spend sats
anywhere on the planet.

参考リンク：btcmap.org/communities

第8章では、ライトニングネットワークを通じて、日常生活の中でビットコインを使う方法について理解を深めました。

ライトニングネットワークは取引をより迅速かつ身近なものとし、ビットコインがレイヤー構造の中で今後どう進化していくのかを示しています。

次の第9章では、ビットコインの技術的な側面を探ります。

暗号技術・ノード・マイナーなど、ビットコインの仕組みをより詳しく見ていきましょう。

第9章： ビットコインの 技術的な 仕組み入門

9.0 はじめに

アクティビティ：「ビットコインの内部構造の仕組み」動画を視聴

9.1 公開鍵と秘密鍵：暗号技術によるセキュリティ

9.1.1 公開鍵／秘密鍵を用いた暗号技術

9.1.2 ハッシュの仕組み

アクティビティ：SHA-256ハッシュの生成

9.2 UTXOモデル

9.3 ビットコインのノードとマイナーの詳細

9.3.1 ビットコインノードとは？ ノードの構築方法

アクティビティ：ビットコインノードに関する動画を視聴

9.3.2 ビットコインマイナーとは？ マイニングはどのように機能するのか

9.4 mempoolとは？

アクティビティ：mempool

9.5 ビットコイン取引の開始から終了までの仕組み

生徒用ワークブック

日本語版 | 2025年版

ビットコインの技術的な仕組み入門

9.0 はじめに

ビットコインは「規制されていない」のではなく、
政府の官僚機構によって規制される代わりに、アルゴリズムによって規制されている。
腐敗していないのだ。

アンドレアス・M・アントノプロス

この章では、ビットコインネットワークが完全に分散された仕組みで動作する技術について、詳しく見ていきます。ビットコインの送金時に何が起こるのか、トランザクションがどのように処理されるのか、そしてネットワークにおけるマイナーとノードの持つ役割を説明します。

この章では少し難しい技術的な概念も扱いますが、覚えておいてほしいのは、「多くの人がインターネットの仕組みを知らなくても、毎日メールを送ったり、SNSで友人と連絡を取ったり、請求書を支払ったりできている」ということです。

ビットコインの技術的な側面の学びは非常に長い旅であり、たとえビットコインをお金として使うと決めた人でも、その仕組みすべてを理解しようと全員が望むわけではありません。

私たちはビットコインの技術的な面について学び続けることを奨励しており、この章では基本的な主要概念に絞って説明していきます。

ビットコイン・プロトコルの仕組み

プルーフ・オブ・ワーク



暗号技術による
タイムスタンプ

難易度調整

ピア・ツー・ピアの
ネットワーク
アーキテクチャ（構造）

ハッシュ関数と
マークリツリー

公開鍵暗号

ブロック報酬と半減期

より深くビットコインの技術について学びたい場合は、このワークブックの巻末に掲載した参考資料を確認してください。

また、私たちのウェブサイトで「Bitcoin Diploma – Technical Edition」に登録すると、技術的なコースの準備が整った際に通知を受け取れます。

まずは、ビットコインネットワークの仕組みを紹介する動画を見てみましょう。

アクティビティ：
[「How Bitcoin Works Under the Hood \(ビットコインの内部構造の仕組み\)」動画を視聴](#)



動画にもある通り、ビットコインネットワークはノードと呼ばれる複数のコンピューターに保存された、取引の台帳または記録に過ぎません。

ビットコインの台帳は擬似匿名性であり、個人情報は含まれず、取引とアドレス情報のみが記録されています。この台帳には、2009年1月3日のネットワーク開始以来のすべてのビットコインと、その移動履歴が記録されています。

第9章

次に、このシステムを可能にしている技術について、より詳しく見ていきます。

9.1 公開鍵と秘密鍵：暗号技術によるセキュリティ

ビットコインが私たちに与えるのは「確固たる約束」である。
プログラムは仕様通りに正確に実行される。

アンドレアス・M・アントノプロス

9.1.1 公開鍵／秘密鍵を用いた暗号技術

暗号技術は、
情報をコードに変換して
秘密を守る技術です。



 暗号化とは、情報を取り込み、特別なコードに変換することで、正しい復号手段を持たない人には読めないようにするプロセスです。これは金庫の鍵を閉めることと似ており、正しい鍵や暗証番号を持つ人だけが開けられます。

 一方、復号とは、暗号化された情報を再び読める状態に戻すことで、金庫を開けて中の情報を読めるようにするのと似ています。

例えば、ジョンがアレルに、他の誰にも読まれたくない秘密のメッセージを送りたいとします。二人はそのメッセージを送る前に、ピッグペン暗号という暗号化方法で内容を隠すことに同意します。暗号を持っている人だけが復号でき、他の人には読めません。

この方法は今日では安全とはみなされていませんが、メッセージを送信するための秘密鍵暗号の原理を示しています。

ピッグペン暗号の解読方法

ピッグペン暗号を解く時、プレイヤーには暗号化されたメッセージと暗号表が渡されます。

メッセージの記号を暗号表で探し、対応する文字を見つけることで復号していきます。

 暗号化されたメッセージの例：

•	—	—							
—	—	—							
A	B	C	J	K	L	S	W		
D	E	F	M	N	O	T	U	X	Y
G	H	I	P	Q	R	V	*	Z	

では、ビットコインの取引において、暗号技術はどのように使われているのでしょうか？

従来の秘密鍵暗号では、ジョンとアレルは最初にパスワードやピッグペン暗号のような、秘密の鍵を共有しておく必要があります。ジョンはその鍵を使ってメッセージを暗号化し、アレルに送ります。

アレルも同じ鍵を知っているので、それを使って復号しメッセージを読むことができます。

しかし、第三者がその鍵を持っていてメッセージを傍受した場合、その人も復号して内容を読むことができてしまいます。

ビットコインの技術的な仕組み入門

ビットコイン取引で使われている公開鍵暗号方式は、この問題を解決しました。

公開鍵暗号では、ジョンとアレルはパスワードや暗号方式を共有する必要はありません。

その代わりに、二人はそれぞれ異なる2つの鍵を持っています。

1つは誰にでも共有してよい「公開鍵」、もう1つは他人に知られてはいけない「秘密鍵」です。

この場合、ジョンがアレルにメッセージを送りたい時は、アレルの公開鍵を使って自分のメッセージを暗号化し、それを送ります。

アレルは、そのメッセージを自分の秘密鍵で復号することで読むことができます。

たとえ他の人がメッセージを傍受しても、読むことはできません。

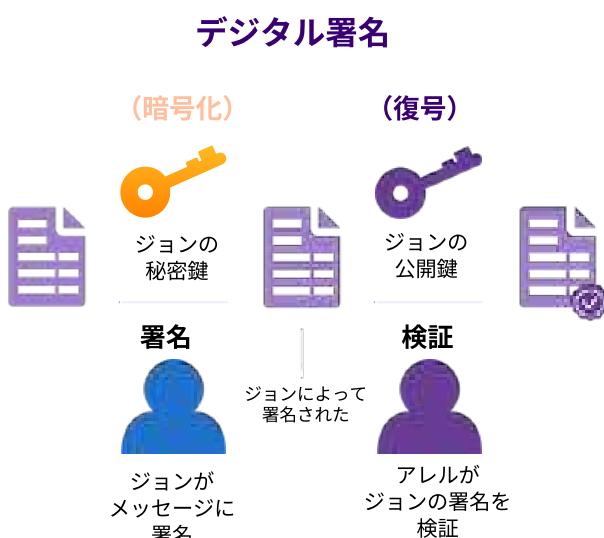
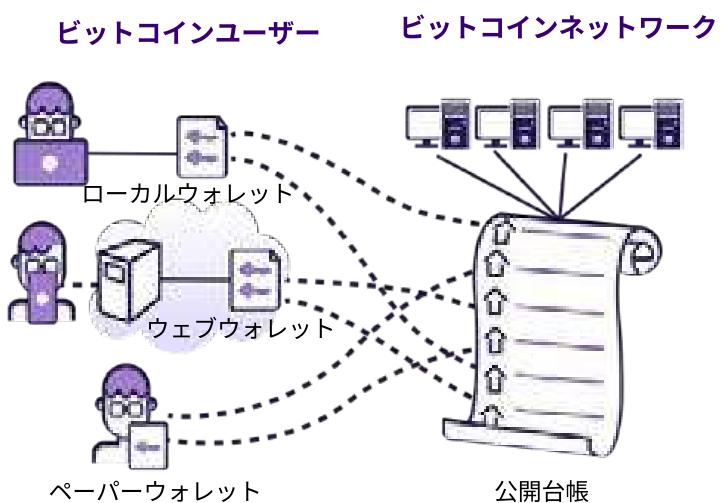
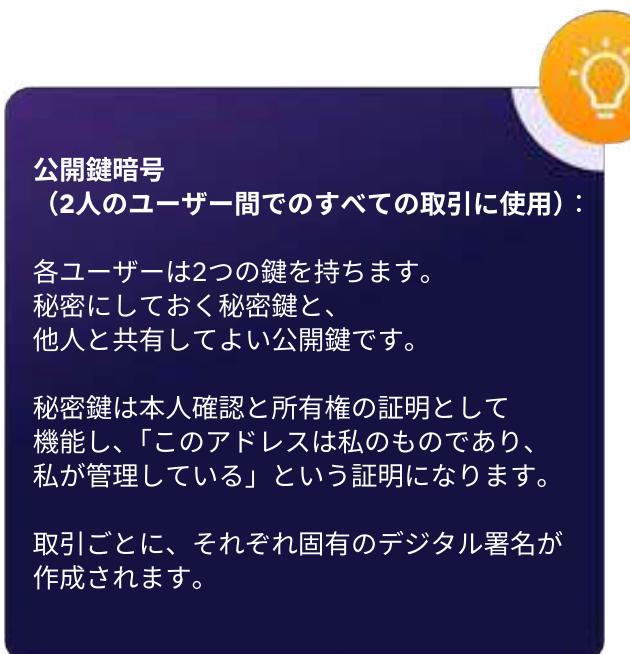
ジョンとアレルが秘密鍵を共有する必要がないため、鍵を盗まれる可能性もはるかに低くなります。

つまり、公開鍵暗号方式の主な利点は、送信者と受信者が最初に秘密の鍵（またはピッグペン暗号のような暗号方式）を共有する必要なしで、安全な通信を可能にする点です。

最初に秘密鍵を共有する場合、第三者に傍受される可能性があります。

ビットコインでは、公開鍵暗号は暗号化されたメッセージを送るために使われるのではありません。ビットコイン取引を不可逆（元に戻せない状態）にするため、固有のデジタル署名を作成するために使われます。

デジタル署名とは、物理的な書類に署名をするように、ビットコイン取引の正当性を証明する手段です。



第9章

◆ ビットコインの取引は、ある量のビットコインを他人のアドレスに直接送信するプロセスです。

◆ 暗号化は、正当な保有者だけがビットコインを送金できることを保証する仕組みとして使われています。
これにより、悪意のある第三者の攻撃から資産を守ることができます。

◆ さらなる保護策として、ビットコインで送信されるすべての取引には、自動的に固有の署名が付きます。
この署名は改ざん防止技術によって強化されており、送信者本人によってビットコインが送られたことをネットワークが確認できるようになっています。

アリス（現金口座）

借方	貸方
	100ドル

ボブ（現金口座）

借方	貸方
	100ドル

公開台帳
(デジタル領収書)

アリス	ボブ
100ドル	100ドル
Out	In
署名	署名

実際のビットコイン取引がどのように機能するか、簡単に説明します。

1 取引の作成：

ユーザーは受信者のアドレスや送金額などの詳細を指定して、ビットコイン取引を開始します。

2

デジタル署名の生成：

送信者は自分の秘密鍵を使って固有のデジタル署名を生成します。
この署名は、取引の正当性を証明する暗号コードです。

3

取引のブロードキャスト：

署名された取引はビットコインネットワークにブロードキャストされ、送信者から受信者への所有権移転の意思をネットワークに伝えます。

4

ネットワークでの検証：

ネットワーク上のノードが取引を受信し、送信者の公開鍵を使って取引の整合性とデジタル署名の正当性を検証します。

5

ビットコインネットワークでの承認：

検証が成功すると、その取引は台帳に追加されます。この台帳は、すべての取引を安全かつ透明に記録する仕組みです。

承認されると、ビットコインの所有権が正式に送信者から受信者に移転されます。



まとめると、送信者の秘密鍵で作られたデジタル署名は、取引の正当性と所有権を暗号的に証明する手段なんだ。

それによって、ビットコインの分散型ネットワークが取引を検証して、台帳に記録できるようになるんだよ。

ビットコインの技術的な仕組み入門

9.1.2 ハッシュの仕組み

これから出てくる難しい専門用語や数学的な概念は、難しそうに見えるかもしれません。構える必要はありません。

数学が得意でなくても大丈夫です。少し努力すれば、複雑な内容も意外と理解できるかもしれません。

関数とは？

関数は情報を受け取り、それを新しいものへ変換する機械のようなものです。関数に与える情報を入力（インプット）、関数が生成した新しい情報を出力（アウトプット）と呼びます。関数はコンピューターがタスクを実行したり、問題を解決したりするのに役立ちます。

サラダのレシピにたとえてみましょう。レシピ（＝関数）は、どんな材料を使い、どう混ぜればサラダができるかを教えてくれます。材料を変えても、レシピを実行した時に得られる出力は必ずサラダです。

関数は物事を簡単かつ効率的にするために使われます。このレシピは、材料を入力として受け取り、混ぜ合わせたサラダを出力として生成する関数です。

ビットコインでも、関数が取引の実行に利用されています。ビットコイン取引は本質的に、あるアドレスから別のアドレスへ価値（お金）を移転する行為です。取引を実行するために、複数の暗号関数が使われ、取引を検証しビットコイン台帳の状態を更新します。

具体的には、取引入力の正当性の検証、送信者の残高確認、関連アドレスの残高更新などを行います。取引が検証され、台帳のブロックに追加されると、その内容はネットワーク上の永久的な記録となるのです。

一方向関数とは？

一方向関数は一連の指示を使用して情報を処理し、新しいものへ変換する仕組みです。

例えるなら、スムージーのレシピが材料を混ぜて新しい飲み物を作るようなものです。

しかし、スムージーを元の材料に戻せないのと同じで、一方向関数を逆にたどって元の情報を取り出すことは極めて困難になります。



第9章

公開鍵暗号は、公開鍵を構成要素とする暗号方式であり、一方向関数の仕組みに依存しています。この関数によって、公開鍵から秘密鍵を逆算するのが非常に困難になっているのです。

理論的には、公開鍵から秘密鍵を見つけることは「完全に不可能」というわけではありませんが、現実的には極めて難しく、途方もない時間と計算能力を要します。

ビットコインにおいて公開鍵から秘密鍵を見つけようとするのは、広大なサッカー場に山のように盛られた干し草の中から針を探すようなものです。

針は秘密鍵、干し草は理論上可能なすべての秘密鍵を表しています。

このように、一方向関数は逆算できないように設計されており、復号化できません。



ハッシュ関数とは？

ハッシュはデジタルデータにおける指紋のようなものです。デジタルメッセージを一定の長さのコードに変換するプロセスであり、それによって一意の識別子（複数の対象から特定の一つを識別するのに用いられる文字列や名称）として機能します。

指紋で人を識別できるように、ハッシュはデジタルメッセージを識別できます。ハッシュはビットコイン取引を含む、多くのアプリケーションで使用されています。

ビットコインにおけるハッシュの使われ方

ビットコインでは、すべての取引が台帳のブロックに追加される前にハッシュ化されます。このハッシュは取引の署名として機能し、その取引が有効で改ざんされていないことを証明します。

もし誰かが取引の文字を1つでも変更しようとすると、ハッシュはまったく別のものとなり、他の人にその変更を知らせます。

セキュリティ確保におけるハッシュの役割

ハッシュは、ビットコインネットワークのセキュリティに不可欠な仕組みです。ハッシュを使用して取引を識別することで、ネットワークは取引の改ざんや不正な変更を検知できます。これにより、詐欺行為を防ぎ、すべての取引が正確に台帳に記録されることが保証されます。

ハッシュ関数は、入力（「メッセージ」または「データ」と呼ばれる）を受け取り、「ハッシュ」と呼ばれる数値表現に変換する、一方向関数の一種です。

このハッシュ出力は入力データに対して固有であるため、入力にほんの少しでも変更があると、完全に異なるハッシュが生成されます。

ハッシュ関数は、秘密の暗号生成機のようなものです。メッセージを受け取り、それを暗号に変換します。



任意の長さのデータ



固定長のハッシュ (ダイジェスト)



ビットコインの技術的な仕組み入門

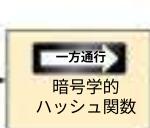
同じメッセージであれば、生成されるコードは常に同じです。

メッセージをほんの少しでも変更すると、コードはまったく異なるものになります。これにより、コンピューターが内容を記憶し、変更が加えられていないかを確認するのに役立ちます。



入力された文字列や値から、瞬時にSHA256ハッシュを生成できるよ。ハッシュ関数は、一方通行の仕組みとして使われているんだ。

アクティビティ： SHA-256ハッシュの生成



Output
d2ca4f53c8257301
86db9ea585075f96
cd6dfbf4fb7c68
7a23b912b2b39bf6
32バイトのハッシュ

ヒゲがない！これじゃあ彼女が不機嫌になっちゃうね。



前のハッシュとはまったく異なるよ。
Output
d2ca4f53c8257301
86db9ea585075f96
cd6dfbf4fb7c68
7a23b912b2b39bf6
A 32-byte hash

出力、つまりハッシュは、元の情報の長さに関係なく常に一定の長さになります。ビットコインでは、SHA-256やRIPEMD160と呼ばれる特定の種類のハッシュ関数が使われています。

例：

2番目の入力のわずかな変更によって、最初の入力と比較して出力が完全に変わる点に注目してください。

3番目の入力は非常に大きなファイルですが、それでも出力は他の2つと同じ固定長です。

- SHA256 hash of the string hello world
- B94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9
-
- SHA256 hash of the string hello world.
- 7ddb227315f423250fc67f3be69c544628dff41752af91c50ae0a9c49faeb87
-
- SHA256 hash of the downloadable iso file Ubuntu 18.10
- 7b9f670c749f797a0f7481d619ce8807edac052c97e1a0df3b130c95efae4765
-

ハッシュは、音楽の本質をとらえた楽譜のようなものだとも考えられるよ。楽譜がそのメロディーの固有さを表しているように、ハッシュ値はデータを固有に表現している。ミュージシャンが演奏と楽譜を照らし合わせて演奏の正確さを確認できるように、受け取ったデータのハッシュ値を元のハッシュ値と比較することで、転送中にデータが改ざんされたかどうかを判断できるんだ。



第9章

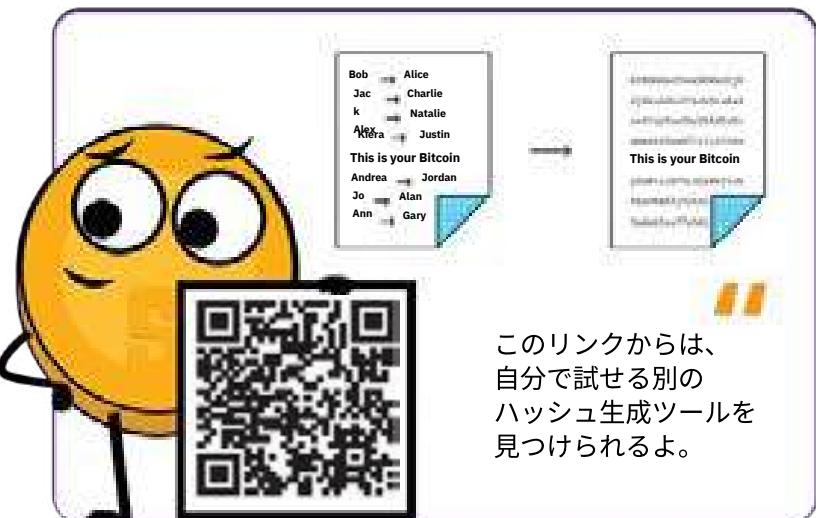
音楽の演奏でわずかなズレがあると違った響きになるように、元のデータにほんの少し変更があるだけで、ハッシュ値はまったく異なるものになります。この特性により、ハッシュ化はビットコイン取引の完全性と真正性を保証する強力なツールとなるのです。

公開鍵をハッシュ化してエンコードするプロセスは、情報を固定長（データの長さがあらかじめ決まっている状態）の判読不能な形式に変換し、セキュリティを高めるために使われます。

ビットコインでは、SHA-256とRIPEMD-160というアルゴリズムを使って公開アドレスを生成します。

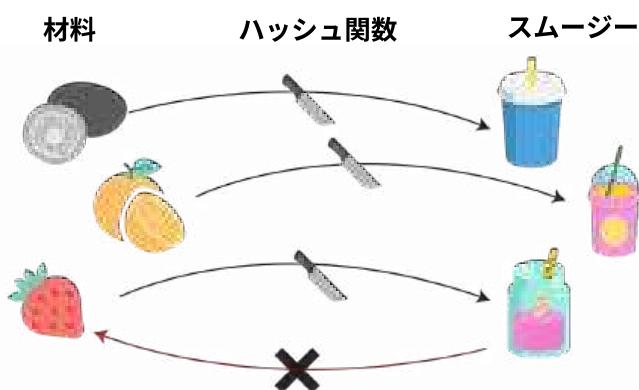
生成される出力は、公開鍵の一意の識別子となり、台帳に保存される取引の整合性とセキュリティを確保するのに役立ちます。

このように情報を処理することで、許可のない者がデータにアクセスしたり操作したりするのがより困難になるのです。



ハッシュ処理

ハッシュ関数は任意の入力を受け取り、固定長の出力（ハッシュ）を生成します。



決定論的：同じ材料を使えば、常に同じスムージーができます。

原像計算困難性：スムージーから元のイチゴを再構成することはできません。

相関耐性：材料を少し変えるだけで、まったく別のスムージーになります。

衝突耐性：異なる材料でまったく同じスムージーを作るのは困難です。

速度と検証可能性：果物をミキサーに入れると、素早くスムージーが出てきます。そして必ずスムージーになります。

9.2 UTXOモデル

UTXO - 未使用のトランザクション出力（Unspent Transaction Output）



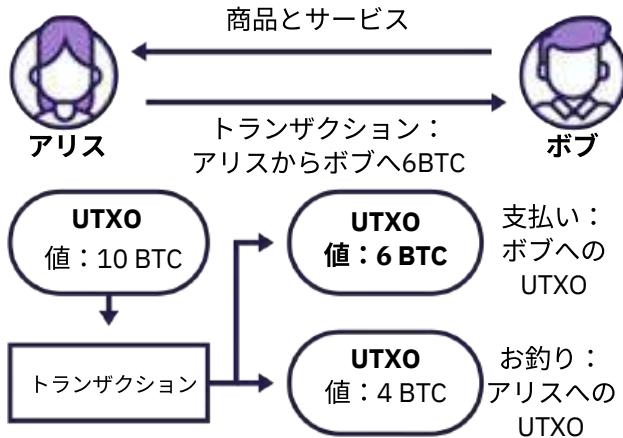
ビットコインの技術的な仕組み入門

UTXOとは？

ビットコインにおける取引は、大きな金の塊を小さなピースに砕き、それらの小さなピースを他者と自分自身に送るようなものです。UTXOは、さまざまなサイズやピースのビットコイン、またはお財布に入っている異なる額面のお札だと考えることができます。

UTXOを使って支払いを行うと、受取人用に新しいUTXOが生成され、残りは「お釣り用UTXO」として、新しいUTXOの形で自分に返されます。これは、1000円札で600円のコーヒーを購入する時、お店に600円を渡して、400円のお釣りを受け取るのに似ています。

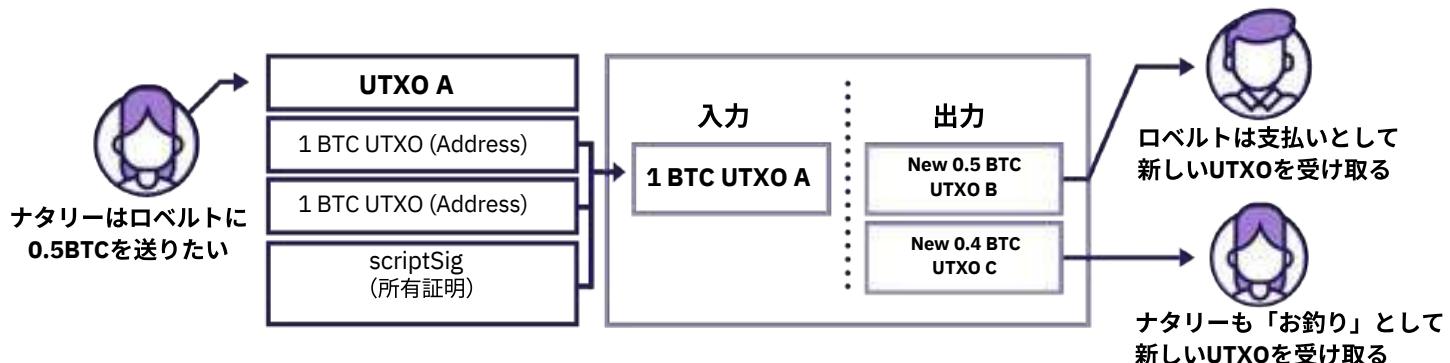
ビットコインを送るときは、ウォレットにあるUTXOの1つ（または複数）を全額送信します。何が起こるかというと、一部は相手に送られ、残りは新しい自分のビットコインアドレスに「お釣り」として戻ってきます。このお釣りは未使用トランザクション出力（UTXO）として、今後の新しい取引の入力として再び使用できます。あなたのビットコインウォレットの残高は、異なるUTXOのすべての合計です。つまり、UTXOの合計額が、あなたの保有するビットコインの総量を表しています。



自分のUTXOを他人に知られないようにすることはとても重要です。
なぜなら、UTXOが知られてしまうと、ネットワーク上であなたのビットコイン取引を追跡でき、最終的にはあなたの保有額を知られる可能性があるからです。



まとめると、取引を行ったびに、手元にあるUTXOを1つ以上使ってビットコインを支払い、送信先と自分用（お釣り）の新しいUTXOが生成されます。



トランザクションが実行されると、送信されたビットコインは複数の出力に分割され、それぞれが新しいビットコインアドレス（新しいUTXO）と関連付けられます。

第9章

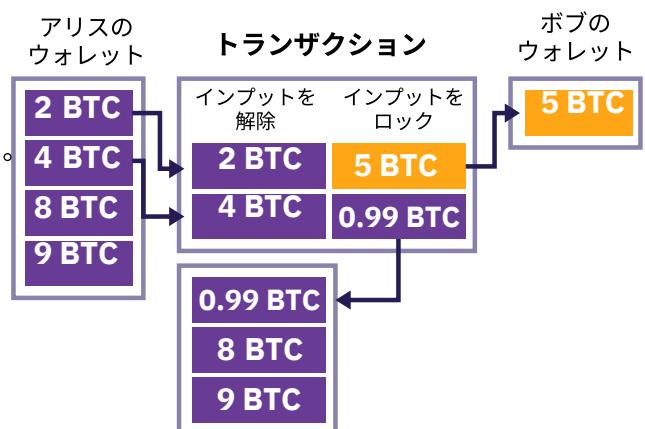
ビットコインを誰かに送金する時は、資金源（インプット）として1つ以上のUTXOを使用します。必要に応じてこれらのUTXOが組み合わせられ、取引の受取人とあなた自身の両方に属する新しい出力（アウトプット）が作成されます。こうしてできた新しい出力、つまりUTXOは、それぞれ受取人とあなたの所有物となるのです。

これらのUTXOは、今後の別の取引でも資金源として使用できます。このUTXOの連なりが、2009年1月3日の最初のブロックから始まるビットコインの台帳上の、すべてのビットコイン取引の透明で追跡可能な取引履歴を作り出しているのです。

例として、「2BTCを送りたいが、5BTC分のUTXOしか持っていない」場合、差額の3BTCは「お釣り」として自分に送り返されます。このお釣りも新しいUTXOとして発行され、次の取引で使用できます。

別の例：

- 1** アリスはボブに5BTCを送りたい。
- 2** アリスは2つのUTXOを組み合わせて6BTCを用意する。
- 3** この6BTCから、アリスはボブに5BTCを送り、0.99BTCを自分へのお釣りとして受け取り、0.01BTCを取引手数料として支払う。
- 4** 承認後、この取引はビットコインの台帳に記録され、台帳のコピーを持つすべてのノードが更新される。



アリスがすでに使ったアウトプットを使って再度取引をしようとした場合、その取引は自動的にノードによって拒否されます。これは、各ノードがビットコインの台帳（およびすべての取引）のコピーを保持しているため、アリスのUTXO残高を簡単に確認でき、その取引が有効ではないことを検証できるからです。

以下の例は、入力が1つしかない実際の取引のスクリーンショットだよ。でも別のケースでは、最初の残高が複数のUTXO（複数のインプット）の合計になっていることもあるんだ。



この2つの取引を見たとき、どんなことに気づけるかな？
インプットとアウトプットは一致してる？取引の詳細を説明できる？
2つのスクリーンショットには何か関係があるかな？それから、どちらの取引が先に行われたと思う？

ビットコインの技術的な仕組み入門

9.3 ビットコインのノードとマイナーの詳細

このセクションでは第6章で紹介された、ビットコインネットワークの中で非常に重要な2つの要素（および参加者）について、より詳しく見ていきます。

1

ビットコインノード

検証の門番としての役割を持ちます。主な仕事はビットコインの台帳（Ledger）のコピーを保持して、すべての取引が有効であり、みんなが同じルールに従っているかを確認することです。この役割が世界中の多くの人々に分散されることで、ビットコインはさまざまな問題に対して耐性を保ち続けます。これらのノードは、特定の個人や組織が過剰な力を持たない、信頼できる分散型システムという理念を守る役割を果たしています。

ビットコインマイナー

2

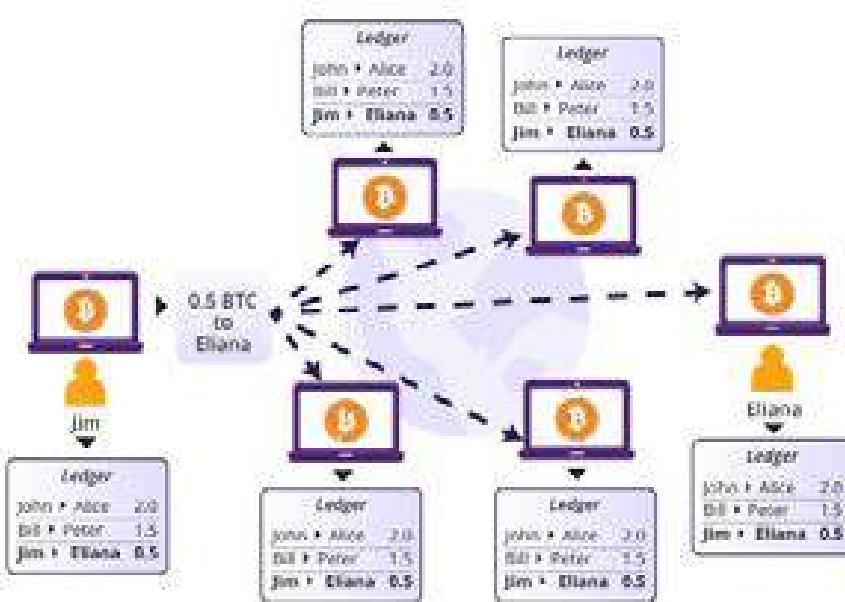
強力なコンピューターと電力をを使って取引をチェック・確認し、ネットワークの安全性を確保する「セキュリティの設計者」です。この作業によって、台帳、すなわちブロックチェーンは、悪意ある攻撃者の妨害行為に対して耐性を持つようになります。

ビットコインのノードとマイナーは協力し、分散型で安全かつ強固なシステムを維持するチームとして機能します。これが、世界中の人々が信頼できる、新しいお金の仕組みなのです。では、これらの役割をさらに詳しく探求し、ビットコインの革新的なシステムにどのように貢献しているかを理解しましょう。

9.3.1 ビットコインノードとは？ ノードの構築方法

ビットコインノードというと技術的に聞こえるかもしれません、実際はビットコインの台帳のコピーを保持し稼働させるソフトウェアにすぎません。あなた自身のビットコインノードを稼働させれば、ビットコインネットワークのルールを形成する上で発言権を得られます。

例えば、あるグループがビットコインの総供給量を変更するなど、ビットコインの仕組みを変えようとした場合、あなたには意思表示の手段があります。自分のノードを新しいシステムに切り替えないという選択は、あなたが支持するネットワークのルールを強制する、投票のような役割を果たすのです。



ビットコインノードを「デジタル交通警察官」として考えてみましょう。そこにはいくつか重要な役割があります：

第9章

検証の門番：

1

ビットコインノードは、すべてのビットコイン取引の共有台帳のような、ブロックチェーンのデジタルコピーを保持します。世界中の多くのノードが同じ記録を保持しています。

コミュニケーションハブ：

2

ノード同士は相互に接続し、広大な通信ネットワークを形成します。ノードは情報を共有し、特に「mempool（メンプール）」と呼ばれるデジタルの待機室に保管される、ブロックチェーンへの追加を待つ取引を共有します。

3

品質チェック係：

ブロックチェーンへの追加はすべて精査されます。ノードは、取引が有効であることを確認し、ビットコインネットワークのルールに従っていない取引を拒否します。

4

ブロックチェーンの情報提供者：

ウォレットなどの他のソフトウェアは、ビットコイン残高などのブロックチェーンに関する情報をノードに問い合わせることができます。ノードは情報のハブとして機能します。

5

新しいノードの案内役：

新しいノードが参加したい場合、既存のノードはブロックチェーンのコピーを惜しみなく提供します。

そして新しいノードは、すべての取引の正当性を自らチェックし、

「トラストレスな（信頼に頼らない）システム」であることを体現します。

アクティビティ：

ビットコイン
ノードに関する
動画を視聴



自分のノードを稼働する方法の1つは、Bitcoin Coreソフトウェアをダウンロードして、時間をかけてブロックチェーン全体を取得することです。準備が整い、ノードを常時稼働すれば、約10分ごとに新しい取引を含むブロックが到着します。あなたのノードはそれらの有効性を検証し、ローカルのブロックチェーンコピーに追加します。

リソース：

Bitcoin Core
ソフトウェア



ノードを稼働させることで、主権と独立性を得られます。あなたは他者に依存せず、独自の「交通警察官」として機能するのです。ブロックチェーンのコピーを持たないビットコインウォレットとは異なり、ノードは自立性を保証します。ビットコイン残高やネットワークの状態について他人を信用する代わりに、あなたのウォレットがあなた自身のノードと直接やり取りすることで、より安全で信頼できるデジタル体験を実現できます。

9.3.2 ビットコインマイナーとは？マイニングはどのように機能するのか

マイニングの目的は新たなビットコインを生み出すことではない。それは単なるインセンティブだ。
マイニングは、ビットコインのセキュリティを分散化するメカニズムである。

アンドレアス・M・アントノプロス

ビットコインの技術的な仕組み入門

マイナーは未承認のトランザクションを集めてブロックを作り、エネルギーを消費してブロックをブロックチェーンに追加し、その位置を確定させるための「貴重な鍵」を探します。



マイナーは、次のブロックをブロックチェーンに追加する競争をしています。

彼らが狙うのは「有効なブロックハッシュ」で、何十億もの組み合わせの中から、ネットワークが定めた条件を満たす唯一の正解を見つけ出さなければなりません。

何百万もの鍵が詰まった巨大な干し草の山を想像してください。それぞれの鍵は固有のブロックハッシュを表します。

ネットワークは貴重な宝箱を開けるための鍵の条件を決めます。マイナーは干し草の山の中を探し回り、1つずつ鍵を試しますが、完璧に合う鍵を見つけられるのは運の良い1人だけです。

正しいブロックハッシュを見つけたマイナーは、それを新たに作ったトランザクションのブロックとともにネットワークに共有します。他のマイナーたちがその解答を検証し、正しければそのブロックはブロックチェーンに追加され、安全で公開された台帳が形成されます。

マイナーは以下の2つの方法で報酬を得ます：

- ① ブロック報酬
- ② トランザクション手数料

ブロック報酬は、ブロックチェーンにブロックが追加されるごとに流通に放出される、新しいビットコインです。トランザクション手数料は、ユーザーが自分のトランザクションをより速く処理するため、マイナーに優先してもらうために支払う少額のビットコインです。

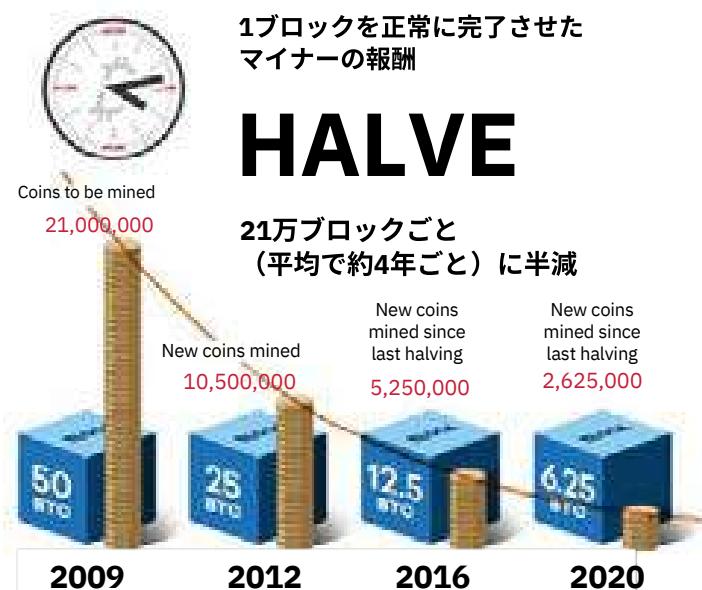
マイナーは、マイニングするブロックにどのトランザクションを含めるかを選択でき、通常は手数料の高いトランザクションを優先します。

ビットコインの半減期

ビットコインの半減期は、ビットコインの希少性と価値を長期にわたって維持する重要な仕組みです。ご存じのとおり、ビットコインの総供給量は2,100万枚と決まっています。この供給量は、ビットコインが誕生した時点で一気に出回ったわけではなく、段階的にビットコインの世界に放出されています。

サトシ・ナカモトは、中央の権力に頼らずに新しいビットコインを配布するために、ブロック報酬の仕組みを巧みに設計しました。

ビットコイン初期には1ブロックあたり50BTCという報酬があり、マイナーが機材や電力に投資する動機の1つとなりました。



ネットワークの安定を保ち、新しいビットコインの供給を管理するために、ブロック報酬は約21万ブロックごとに半減されます。

このイベントは「半減期 (halving)」と呼ばれ、新しく流通するビットコインの数を減らすことで、マイナーに対してネットワークを守り、分散性を維持するモチベーションを与え続けています。

過去の傾向として、半減期によって新しいビットコインの供給が減った影響で、市場では大幅な価格上昇が見られました。

第9章

流通供給量とは、ある通貨の総量を指します。

ビットコインにおける総流通供給量とは、これまでにマイニングされ、現在流通しているコインの総数です。

ただし、失われたと考えられるコインが含まれている場合もあります。

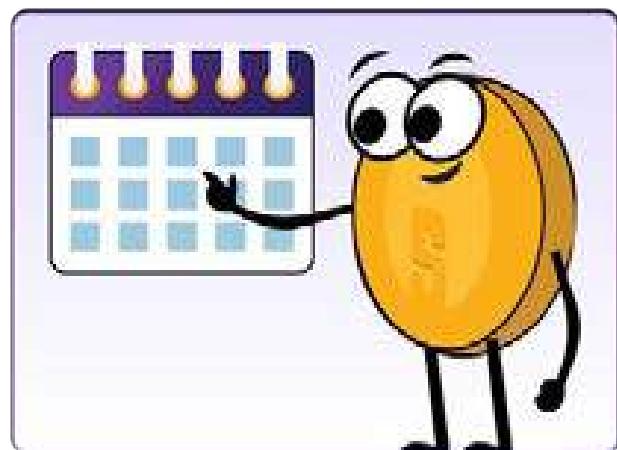


それぞれの半減期イベントでは、マイナーが受け取るビットコインの報酬が減少し、新しいコインの発行速度が下がります。その結果、約10分のブロック生成時間を維持するために、ビットコインのマイニング難易度が上昇し、新しいブロックが安定したペースでブロックチェーンに追加されるように調整されます。

マイニング報酬の減少は、必ずしもマイナーの利益が減ることを意味するわけではありません。

なぜなら、マイナーはトランザクションを検証してブロックチェーンに追加することで、トランザクション手数料も得られるため、報酬減少を補える可能性があるからです。

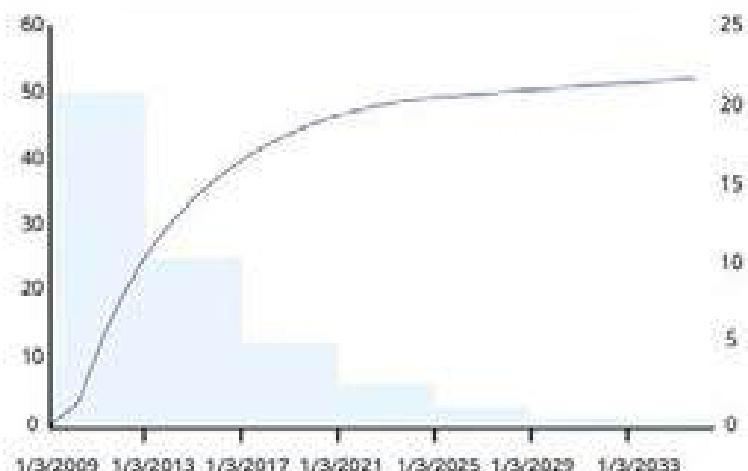
半減期イベントはビットコインのプロトコルにあらかじめ組み込まれており、ビットコインの供給スケジュールは予測可能で透明性があります。



ビットコインの供給スケジュールは、新しいビットコインを流通させるためにあらかじめ定められた公開計画であり、長期的にビットコインの希少性を保つように設計されています。

以下の表は、今後予定されているビットコインの半減期イベントの詳細です。今後の半減期の予想日、半減期が発生するブロック番号、期間中のブロック報酬、および総供給量の何パーセントがマイニングされるかが示されています。

ビットコイン供給スケジュール



イベント	予想日	ブロック番号	ブロック報酬	マイニングされた割合
第4回半減期	2024	840,000	3.125	96.875 %
第5回半減期	2028	1,050,000	1.5625	98.4375 %
第6回半減期	2032	1,260,000	0.78125	99.21875 %

ビットコインの技術的な仕組み入門

より多くのビットコインがマイニングされるにつれて、流通供給量と、総供給量に占めるマイニング済みの割合は、最終的に2,100万枚に達するまで増加し続けます。

供給の減少と需要の増加が相まって、ビットコインの価格（ドルや円に対する価値）が上昇する可能性があります。

これは初期の導入者に利益をもたらすとともに、マイナーが引き続きネットワークを保護し、計算能力とリソースを提供し続ける動機付けになります。

ビットコイン：2,100万枚中のマイニング済み割合



ビットコインにおける有効なブロックハッシュとは？

ビットコインにおいて、有効なブロックハッシュはマイナーが見つけようとする特別なコードのようなものです。これは、トランザクション情報を保存するブロックチェーンの各ブロックを識別・検証するのに役立つ、一意の値です。

ブロックは、最初のブロック（ジェネシス・ブロック）から最新のブロックまで鎖のようにつながっており、すべての取引の公開記録を形成します。このブロックハッシュは、各ブロックをその前のブロックにリンクさせており、取引の履歴を確認する際に非常に重要です。

ブロックハッシュは「指紋」のような役割を果たし、情報の正確性と安全性を保証します。

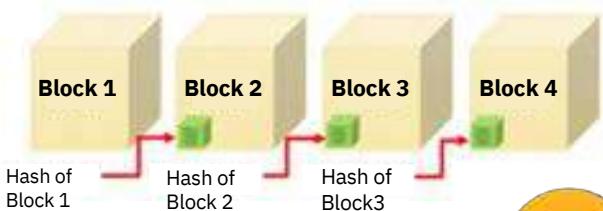
また、ブロックハッシュはブロック内のデータが改ざんされていないことを確認する手段として機能します。



ブロックは、ブロック間の特定の関係を強制することで「リンク」されています。

つまり、各ブロックには、前のブロックのハッシュ値という「指紋（フィンガープリント）」が含まれていなければなりません。

ハッシュ関数は、任意のメッセージ（ブロック情報）を固定長（例：256ビット）のデータに変換し、そのメッセージのフィンガープリントを生成します。



ビットコインの生みの親であるサトシ・ナカモトは、合計50ビットコインを含む最初のブロックをマイニングしました。



第9章

ブロックをマイニングする競争

ビットコインのマイナーは、ネットワークが設定したターゲット（特別な数値）に合致するブロックハッシュを見つけるために競争します。

最初に正しいブロックハッシュを発見したマイナーは、そのブロックをブロックチェーンに追加し、対応するハッシュIDを割り当てる権利を得ます。この解（ハッシュ値）は、ブロックの有効性を証明してくれるのでです。

マイニングは、できるだけ早くゴールに到達することを目指すレースに例えられます。

ブロックハッシュの発見難易度は定期的に調整され、マイナーの数が増減しても、約10分ごとに新しいブロックが生成される仕組みです。

このメカニズムは「難易度調整（difficulty adjustment）」と呼ばれます。



例えば、ビットコインネットワークが設定したターゲット値が1,000だとします。

マイナーは計算能力と電力を使って、この1,000よりも小さいブロックハッシュ（特定の数値）を探さなければなりません。

最初に1,000未満のブロックハッシュを見つけたマイナーが、新しいブロックをブロックチェーンに追加し、ビットコインの報酬を受け取れます。



ビットコインのマイニングにおける「マイニング難易度」とは、ネットワークが設定したターゲットを満たす有効なブロックハッシュを見つけることが、どれだけ難しいかを示す指標です。

この難易度は2,016ブロックごと（約2週間ごと）に調整され、ブロックが一定のペースでブロックチェーンに追加されるように保たれています。

難易度は数値で表され、その数値が高くなるほど、有効なブロックハッシュを見つけるのはより困難になります。

例えば、以下の2つのハッシュを比較してみましょう：

 **ハッシュ1** : 0000A1mINgF0RbL0cK5wItHth3hAy5tAcK

マイニング難易度：1

 **ハッシュ2** : 00000000A1mINgF0RbL0cK5wItHth3hAy5tAcK

マイニング難易度：2

この例では、ハッシュ2の方がハッシュ1よりもマイニング難易度が高くなっています。

なぜなら、先頭にあるゼロの数が多く、より小さい数値として扱われるため、条件を満たすのが難しいからです。マイナーがハッシュ2を見つけるには、より多くの計算処理が必要となるため、難易度が高くなります。



有効なブロックハッシュを見つけることで、マイナーはそのブロックをブロックチェーンに追加するために必要な作業を行ったことを証明します。

その対価として、マイナーはビットコインの報酬とトランザクション手数料を受け取ります。

この仕組みは「プルーフ・オブ・ワーク（Proof-of-Work／PoW）」と呼ばれ、ビットコインネットワークが取引を検証し、新しいブロックを追加する際に使われるメカニズムです。

ビットコインの技術的な仕組み入門

PoW（プルーフ・オブ・ワーク）は、悪意のある人物がネットワークを支配するのを困難にすることで、ビットコインの安全性を保っています。

まとめると、マイナーの作業内容は以下の通りです：

1 トランザクションをブロックにまとめる：

ノードが「mempool」にある未確認トランザクションを検証している間、マイナーはその一部を選び、候補ブロックに含めます。

2 プルーフ・オブ・ワーク：

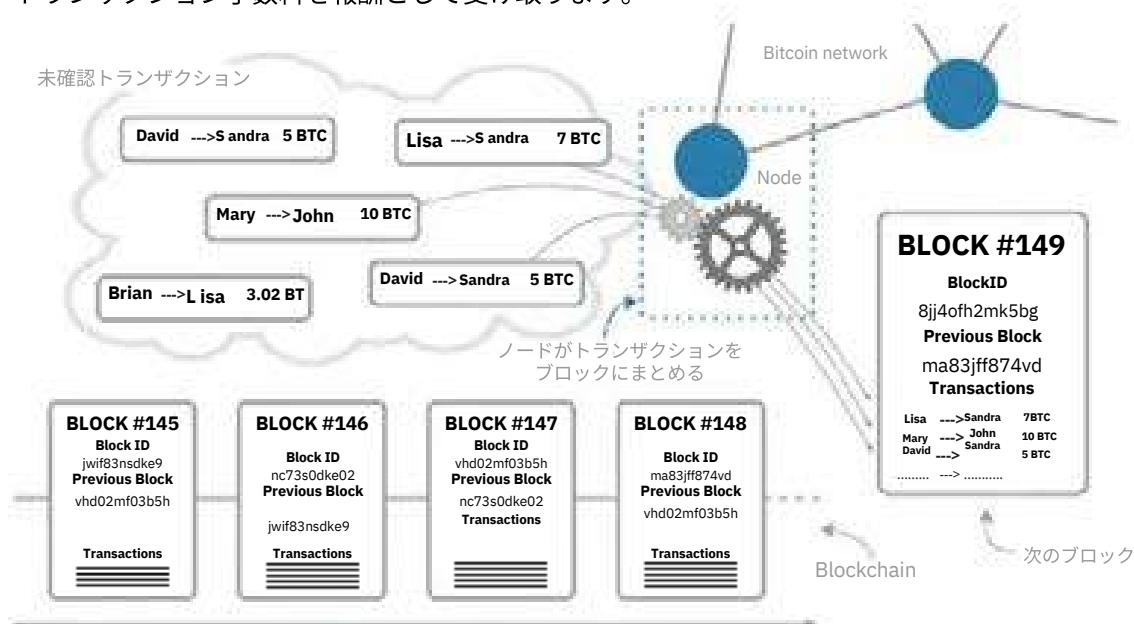
マイナーは有効なブロックハッシュを見つけるために競争します。

3 有効なブロックをブロードキャスト：

有効なブロックハッシュが見つかると、ブロック全体をネットワークにブロードキャスト（送信）します。

4 報酬を得る：

ブロックをブロックチェーンに追加できたマイナーは、新規発行されたビットコインと、そのブロック内のトランザクション手数料を報酬として受け取ります。



複数のマイナーが同時に新しいブロックの作成に取り組むことができます。

ネットワークが設定したターゲットに合致するブロックハッシュを最初に見つけたマイナーは、そのブロックをネットワークに発表します。

他のマイナーたちは、その候補ブロックに含まれるトランザクションが有効かどうかを確認します。

トランザクションが有効であれば、そのブロックはブロックチェーンに追加されます。

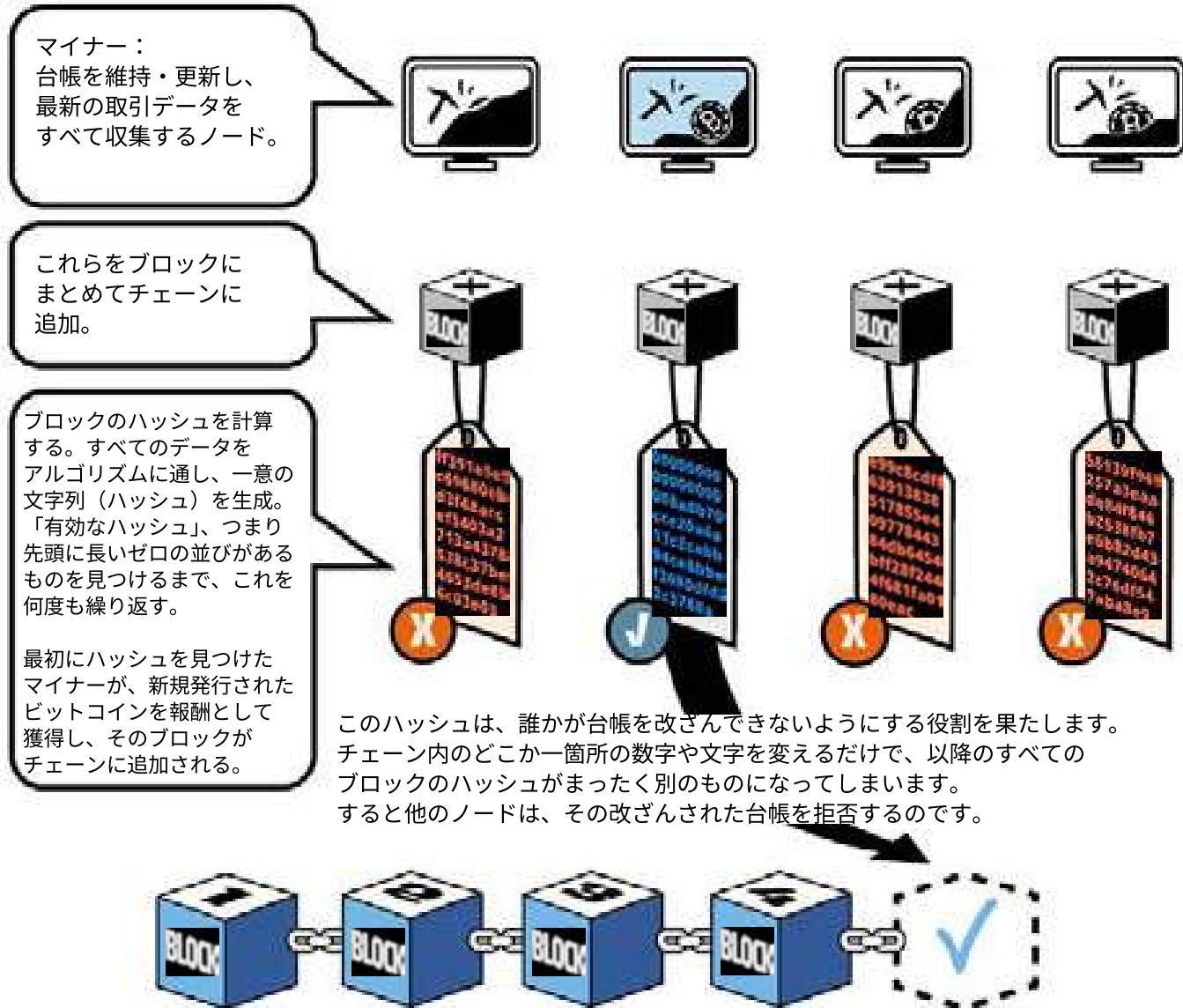
他のマイナーたちが同時に作成していたブロックは採用されず、破棄されます。

この仕組みによってネットワークの合意が保たれ、二重支払いが防止されるのです。

候補ブロックとは、まだブロックチェーンに追加されていないものの、追加候補となっているトランザクションの集合のことです。



第9章



9.4 mempoolとは？

「mempool（メンプール）」は、ビットコインネットワークにおけるトランザクションの待機室のようなものです。トランザクションを行うと、まずmempoolに送られ、検証・選択されてからブロックチェーンに追加されます。

レストランで順番待ちをしている場面を想像してみてください。あなたの名前はテーブルを待つ人のリストに追加されます。テーブルが空いたら店員があなたの名前を呼び、席へ案内します。

同様に、ビットコイントランザクションは作成された時点ではmempoolに追加され、マイナーによってブロックに含まれることで、確認されてブロックチェーンに記録されるのです。

ビットコインの技術的な仕組み入門

mempool（メンプール）は、トランザクションがブロックに取り込まれて承認されるのを待つ場所です。

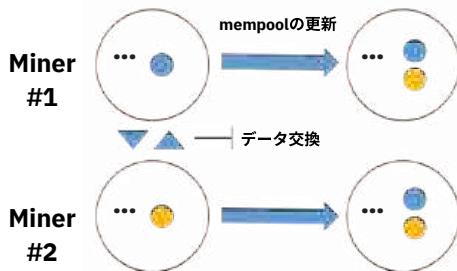
tx hash 6053b699...	fee rate: 3 sat/vB
tx hash bb3b8c8f...	fee rate: 1 sat/vB
tx hash d7c2532a9...	fee rate: 15 sat/vB
tx hash 0ecd9c6...	fee rate: 2 sat/vB



ノードがピア（他のノード）から最初にトランザクションを受け取ったとき、そのトランザクションが正当であるかどうかを検証する必要があります。不正・詐欺的なトランザクションは、誰も受け入れたくないからです。



mempoolの同期によって、ノードは mempool内の検証済みトランザクションのリストを含むメッセージとして送信し、他のノードとトランザクションを共有できます。



トランザクションはどのように検証され、mempoolに追加されるのか？

新しいトランザクションがビットコインネットワークにブロードキャストされると、ノードはそれらが有効であり、以前に使われた資金でないことを確認します。

検証が完了すると、ノードはそれらのトランザクションをmempoolに追加します。

その後、ノードはそのトランザクションを他のノードと共有して、二重チェックを行います。

最終的に、大多数のノードが合意すれば、それらのトランザクションはマイナーが選んでブロックに含められる対象となるのです。

ただし、トランザクションが72時間以上経っても確認されない場合は、いくつかの理由が考えられます：

mempoolの主な目的は以下の通りです：

1

未確認のトランザクションを中継する。

2

マイナーにマイニングするトランザクションを提供する。



mempoolへの受け入れ処理 (ATMP) では、以下のような点がチェックされます：

- ・このトランザクションはすでに保有していないか？
- ・mempool内の他のトランザクションと矛盾していないか？
- ・出力（アウトプット）に対して、入力（インプット）されたビットコインの額が十分であるか？
- ・署名によって、前回の出力が使えることが証明されているか？
- ・十分な手数料があるか？

第9章

手数料が低い場合：

1 手数料が低いトランザクションは処理が遅くなる可能性があります。マイナーは、自分のブロックに含める際に、手数料の高いトランザクションを優先的に選ぶ傾向があるためです。

ネットワークの混雑：

2 ネットワークが混雑している場合、手数料が高くてもトランザクションの確認に遅れが生じることがあります。

二重支払いの試み：

3 悪意のある人物が二重支払いを試みた場合、そのトランザクションはネットワークによって拒否されることがあります。

不正確または不完全なデータ：

4 トランザクションに誤った情報や不完全なデータが含まれている場合、ネットワークによって拒否されることがあります。

不正な形式のトランザクション：

5 形式に問題があるトランザクションは、ネットワークによって拒否されることがあります。

トランザクションが拒否されないようにするために、適切な時間内に処理されるだけの十分な手数料を設定し、送信前にすべてのトランザクションデータが正しいかを再確認することが推奨されます。

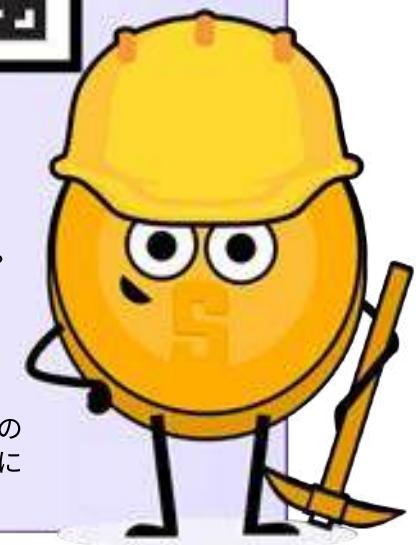
アクティビティ：mempool

1 以下のQRコードをスキャンしてみよう。

2 ページには、最新のブロック、承認されたトランザクション、トランザクション数、メモリ使用量、ブロック全体のおおよその価値などが表示されているよ。
それらを確認して、次の質問に答えてみてね。



- ◆ 最後にマイニングされたブロックの番号は？
- ◆ そのブロックにはいくつのトランザクションが含まれていた？
- ◆ ビットコインで取引された総額はいくら？
- ◆ ブロックのサイズ (MB) はどれくらい？
- ◆ そのブロックのナンス (nonce) は、先頭にいくつのゼロを含んでいる？
- ◆ マイナーが得たビットコインの総額はいくら？
- ◆ マイナーがトランザクション追加の報酬として受け取った、トランザクション手数料の総額はいくら？
- ◆ そのブロックの中で、いちばん価値が高かったトランザクションのひとつを選んでみよう。その金額は何個のビットコインアドレスにわかれていった？



ビットコインの技術的な仕組み入門

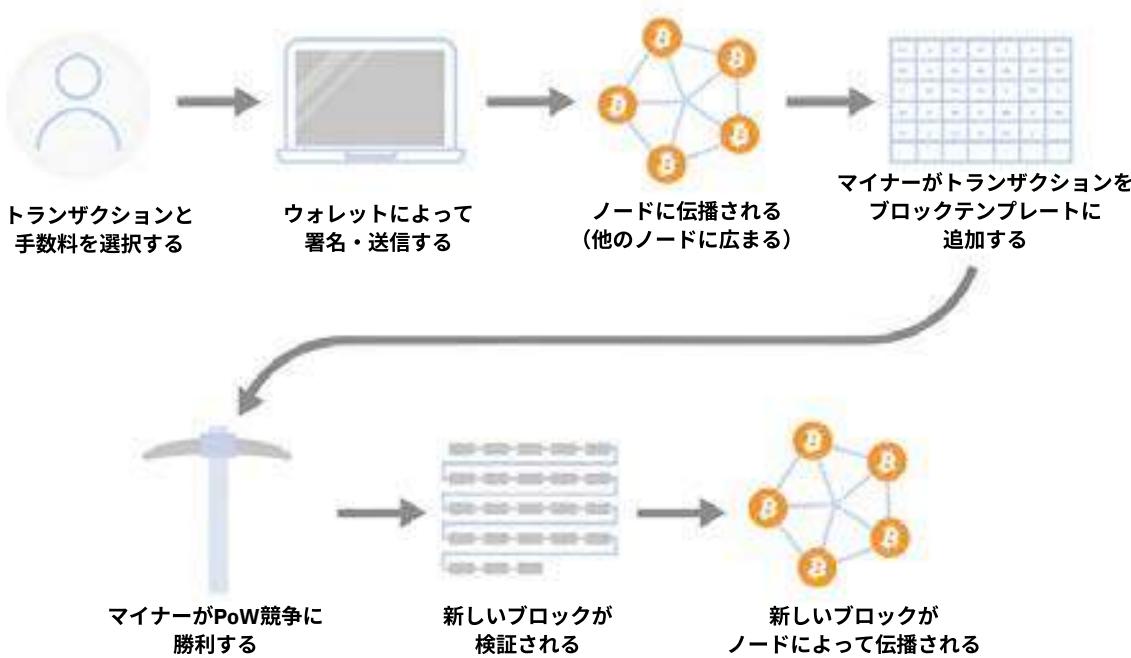
9.5 ビットコイン取引の開始から終了までの仕組み

アダムはジェラルドにビットコインを送りたいと思っています。

- 1 彼は自分のUTXOの1つを選び、トランザクションを作成し、送りたいビットコインの金額、ジェラルドの受取用アドレス、そして平均より高いトランザクション手数料など、必要なすべての情報を追加します。

- 2 すべての詳細が正しいことを最終確認した後、アダムは秘密鍵を使ってトランザクションに署名します。

- 3 そのトランザクションをビットコインネットワークにブロードキャストします。



From: Stevenot, Ted, "What is a bitcoin node and how does one work?". Unchained Capital, 17, January, 2023, <https://unchained.com/blog/what-is-a-bitcoin-node/>

- 4 ネットワーク上のノードはそのトランザクションを受け取り、コンセンサスルールに従って有効性を検証します（一例：アダムの署名が有効か、トランザクションを実行するのに十分な資金があるか）。

- 5 トランザクションが有効と判断されると、ノードはそれを他のノードへと伝播し、mempoolに追加します。

- 6 アダムは十分に高い手数料を設定していたため、ほとんどすべてのマイナーが彼のトランザクションをブロックに含めようとします。

第9章

- 7 プルーフ・オブ・ワーク (PoW)：マイナーたちは競い合い、有効なブロックハッシュを見つけて自分のブロックをマイニングしようとします。
そのうちの1人がハッシュを見つけ、自分のブロックをネットワークにブロードキャストします。
- 8 ノードは新たにマイニングされたブロックを受け取り、その有効性を検証します。
この検証には、ブロック内のすべてのトランザクションが正しいかどうか、プルーフ・オブ・ワークの条件が満たされているかどうかを確認する作業が含まれます。
- 9 多数のノードがそのブロックを有効と認め、ブロックチェーンに追加します。
ジェラルドは、受取用アドレスでビットコインの着金を確認します。
- 10 その後1時間ほどで追加のブロックがブロックチェーンに加わるにつれて、トランザクションの承認回数は増えていきます。
承認回数が増えることで、ジェラルドはトランザクションの成功と取り消せない性質により強い確信を持つようになります。

まとめると、送信者は自分の秘密鍵でトランザクションに署名し、ノードがそのトランザクションのUTXOを検証し、マイナーが検証済みトランザクションをブロックチェーンに追加します。
その後、受信者は自分の秘密鍵を使ってビットコインにアクセスできます。
ブロックがマイニングされると、その中に含まれるすべてのトランザクションは「承認済み」、インプットとして使われたUTXOは「使用済み」とみなされ、二度と使われることはありません。



第9章では、ビットコインの仕組みに関する重要な基礎知識を身につけました。

ここまで、お金の基本からビットコイン技術の技術的な側面まで、欠かせない要素を一通り学んできました。それでは、次の章ですべてをまとめましょう。

第10章では、「なぜビットコインなのか？」という重要な問いに深く迫ります。

第10章： なぜ ビットコインなのか？

10.0 はじめに

アクティビティ：ビットコインの未来はどのようなものになるだろうか？

10.1 中央銀行デジタル通貨（CBDC）とは？誰が管理しているのか

10.2 ビットコインの哲学

アクティビティ：クラスディスカッション — あなたには自分のお金を管理する権利があるか？

10.3 ビットコインの利点

10.4 力を得た未来

アクティビティ：クラスディスカッション — あなたの視点はどう変わった？

生徒用ワークブック

日本語版 | 2025年版

なぜビットコインなのか？

10.0 はじめに

ビットコインは単なる通貨ではない。
人々に力を取り戻す革命であり、変革を渴望するこの世界に、
平和と自由の感覚を与えてくれるものである。

My First Bitcoin

この最終章では、これまでの学びを振り返りながら、いくつかの重要な問い合わせて議論し、ビットコインの未来を探求します。

ビットコインは単なる技術ではなく、誰にも供給量を変えられない、新しい形のお金を動かすネットワークです。人類はこれまで、供給量が固定され、中央集権的な管理のないお金を持ったことがありませんでした。もし広く普及すれば、ビットコインは世界中の人々の生活を変える、ポジティブな変革のムーブメントを解き放つツールとなるでしょう。それは、自由と平等をめざす平和的な革命であり、グローバルで共通の金融システムをつくることで、人類に新たな可能性を切り開いてくれます。

ビットコインは分散型のグローバルシステムとして、少数の者から多数の者へと力をシフトさせ、より大きな金融の自由を可能にします。価値を保存・送信するための安全で検閲に強いプラットフォームとなり、個人が自分の資産を守り、購買力を保持する手段を提供してくれます。これは、従来の金融システムがかつてない困難に直面し、不確実な経済状況の現代において特に重要です。

アクティビティ：ビデオを見てみよう！

ビットコインがもたらすポジティブな変化の可能性は計り知れないよ。
だから、もっと知るためにこのビデオをぜひ見てみてね。



次に、「中央銀行デジタル通貨（CBDC）」と呼ばれるもう一つのデジタル通貨の形を見ていき、ビットコインとの類似点と相違点を評価します。

第10章

10.1 中央銀行デジタル通貨（CBDC）とは？誰が管理しているのか

中央銀行デジタル通貨（CBDC）は、通常の法定通貨をデジタル化したものです。

CBDCは通常の法定通貨と同じルールに従い、政府のような中央機関が新たに通貨を発行することで人々の購買力を低下させます。

そしてCBDCは政府に対し、世界中の人々がお金をどのように使うかを制御するための、新しい強力なツールも与えます。

HRF（ヒューマン・ライツ・ファウンデーション）の調査によれば、世界193か国中119か国の政府が、CBDCを調査・試験運用・導入しているとのことです。

あなたの国がCBDCを試しているかどうかは、HRF（ヒューマン・ライツ・ファウンデーション）のCBDCトラッカーで確認できます。

<https://cbdctracker.hrf.org/home> or
<https://cbdctracker.org/>



では、CBDCはデジタルであること以外に、通常の法定通貨と何が違うのでしょうか？

重要なのは、紙幣や硬貨とは異なり、CBDCは政府が世界中のすべての取引をデジタルで監視・制御できるという点です。



つまり、政府が特定の取引を停止したり、あなたのお金の使い方やあなた自身を気に入らない場合、あなたの口座全体を凍結したりすることも可能になるのです。

例えば、支援を必要とする国に住む家族に送金しようとしても、あなたの国の政府がその国の指導者に反対しているという理由で取引が却下されることがあるかもしれません。

また、店で好きなものを買おうとしても、あなたがSNSで発信した意見が原因で購入できなくなる可能性もあります。

CBDCは政府に、世界中でお金がどのように使われるかを制御する無制限の力を与え、個人が自分の意志でお金を使う自由を制限してしまいます。

中には、「CBDCがあれば、権力を持った政府が人手を介した執行機関を必要とせず、スイッチ一つで地球規模の専制的な政策を強制できてしまう」と主張する人もいます。

CBDCとビットコインはいずれもデジタル通貨ですが、それ以外の点ではまったく異なる思想に基づいたお金であり、人類にとってまったく違った未来をもたらす存在なのです。



なぜビットコインなのか？

10.2 ビットコインの哲学

第6章と第9章で学んだように、ノードを運用する個人は、ビットコインのルールを安全に保つ手助けをしています。これは非常に重要なことです。なぜなら、私たちのような普通の人々が、初めて金融システムのルールを守るチームの一員になれるからです。

ルールの一例として、お金の総量が限られており、誰か一人の権力者がそのルールを変更できないということが挙げられます。

一般の人でも、自分たちのお金の安全性と信頼性を守る役割を果たせる、他に類を見ない機会なのです。

ビットコインの哲学は、エンパワーメント・自由・経済的自立・批判的思考、そして私たちが自分たちのために選んだシステムのルールに対して誰もが発言権を持つべきだという考え方に基づいています。中央集権的な権力が支配する法定通貨システムとは異なり、ビットコインはいかなる単一の主体も完全な支配権を持たないネットワーク上で動作します。つまり、CBDCのような他の通貨と違って、誰かがあなたの財産を奪ったり、お金の使い方を制限したりすることはできないのです。

法定通貨の世界では、より多くの富を持つことが、より大きな影響力や支配力に直結します。

それに対して、ビットコインは人々に力を与えることに重点を置いて機能します。

資産の多少にかかわらず、誰もがシステムの中で重要な役割を担うチーム活動なのです。

例えば、経済的に大きな力を持っていても、すべてをコントロールできるわけではないという、集団的な力をイメージしてください。ビットコインは不变のルールの上に成り立っており、この調和の中で、人類全体がシステムを管理しているかのようです。決定権を持つ少数の権威者が指示を出すのではなく、すべての人が協力し合い、一つの権力に依存することなくビットコインの進路を導いています。

法定通貨システムでは力を持つ者がルールを決めますが、ビットコインのエコシステムでは個人の集合的な力がネットワークを支えています。どれだけの富を持っていようとも、ビットコインのエコシステムの進む道を1人で決めることはできません。

これは、従来の権力構造を逆転させるものであり、システムの強さは少数の者が握るのではなく、すべての参加者の集合的な力にこそあるのです。

その根本的な理念は、誰もが平等にグローバルなお金へアクセスできる、安全で明確かつ公平なシステムを築くことです。

アクティビティ：クラスディスカッションーあなたには自分のお金を管理する権利があるか？

1 お金は人間にとって必要不可欠であり、人権といえるのでしょうか？その理由も考えてみましょう。

2 もし自分の欲しいものを買えず、送りたい人に送金できず、新しい国へ移るときに持つていけないとしたら、そのお金は本当に「あなたのもの」と言えるでしょうか？その理由も考えてみてください。

3 なぜ物々交換は使われなくなったのでしょうか？「欲求の二重の一致」がどんな問題を生むのかも考えてみてください。

4 あなたにとって最も印象深い歴史的な出来事は何ですか？ニクソン・ショックを理解することが、現代の私たちにとってなぜ重要なのでしょうか？

5 供給量が固定されたお金は、従来の法定通貨とどう違うのでしょうか？

第10章

- 6 ビットコインはいつ、誰によって、どのような目的で作られましたか？この目的は、分散型システムの概念をどのように形作っているのでしょうか？
- 7 カストディ型ウォレットとセルフカストディ型ウォレットの違いは何ですか？あなたのお気に入りのウォレットはどれでしたか？
- 8 ライトニングネットワークについてどのように理解していますか？どのような種類の取引に使うのが良いと思いますか？
- 9 自分でノードを運用することが、なぜネットワークをサポートすることになるのですか？
- 10 自分のお金を自分で管理できることは、日常生活や将来の計画にどのような力を与えてくれますか？
- 11 経済的自由は、地域社会や社会に積極的に貢献する力をどのように高めることができるでしょうか？

10.3 ビットコインの利点

「ハイパービットコイン化（Hyperbitcoinization）」とは、ビットコインが世界の主要な金融システムとなるという、仮説上の未来を指します。

つまり、コーヒーの購入から公共料金の支払い、さらには不動産の購入に至るまで、あらゆる場面で誰もがビットコインを使うようになるということです。

個人・企業・国家・政府の間でビットコインへの関心が高まっていることは、その普及が経済や社会に変化をもたらす可能性を示しています。以下に、ハイパービットコイン化された世界のいくつかの利点を示します。

自己主権の未来：

- 1 自己主権の未来とは、世界中の個人が自分のデジタルアイデンティティと資産を完全にコントロールできる状態を指します。これにより、金融包摶・自由・プライバシー・セキュリティが向上し、人類の繁栄・経済的な豊かさ、そしてより良い暮らしの実現につながる可能性があります。

信頼できる価値の保存手段：

- 2 ビットコインはデジタルな希少性を持つため、信頼できる価値の保存手段となります。これにより、より多くの人々が将来のための貯蓄手段としてビットコインを利用するようになるかもしれません。

金融政策の変化：

- 3 もしビットコインが広く普及すれば、政府が従来の金融政策の手段を通じて通貨供給量をコントロールする力を失う可能性があります。ビットコインの大規模な普及は、人々の購買力を高め、社会全体が長期的視点を持った行動へと向かうように促すかもしれません。

透明性と追跡性の向上：

- 4 ブロックチェーン上に記録される改ざん不可能で不变の取引履歴は、さまざまな業界や分野において透明性と説明責任を高める可能性があります。現在では、強大な組織が世界中で数兆ドル規模の資金を動かしても、それがどこへ行き、どのように使われたのか明確に見えないことがあります。ビットコインは、資本の流れに説明責任をもたらし、一般の人々にも透明性を確保する手段となるのです。

なぜビットコインなのか？

送金市場における革命：

5

送金市場とは、一方の当事者からもう一方へ、特に国境を越えて資金を送ることを指します。コストは徐々に下がっているものの、送金は国内の銀行送金に比べて依然として割高であり、特に小口送金はその傾向が顕著です。

ライトニングネットワークは、高速で安価な取引を提供するため、送金市場に非常に適しています。高コストや決済の遅延、営業時間の制限といった、送金に伴う他の課題解決にもつながります。

豊富なエネルギー：

6

安価で豊富なエネルギーがある時、社会はより良く発展し、家庭・企業・新技術における電力需要の高まりにも対応できます。

ビットコインのマイニングは、太陽光・風力・水力などの持続可能なエネルギーから発生する、通常は無駄になる余剰電力を有効活用するよう、マイナーにインセンティブを与えます。

マイナーは余剰エネルギーを使ったマイニングを通じて新たなビットコインを生成し、ネットワークを保護し、さらにそのエネルギーの一部を必要に応じて社会の電力網に還元することもあります。

10.4 力を得た未来

ビットコインはお金です。

お金は、社会において何が重要な活動・商品・サービスなのかを、人々が互いに伝え合うのに役立ちます。本コースでも見てきたように、お金が中央集権的な権力によって管理されると、それは必ず操作されます。

人類が歴史の中で繰り返してきた過ちは、お金の操作であり、それによって個人・家族・企業・政府、ひいては人類全体の繁栄に悪影響を与えてきました。

これは、根本的に異なる世界です。

中央集権的な主体からお金の支配を取り上げ、誰にも変更できない供給量を持つお金を用いることで、私たちは異なる世界を創造できます。

それは「人が正しいことをすると信じる」必要のある世界ではなく、「人が間違ったことをできないように設計された」世界です。

そしてあなたも、この世界をつくる一員になれます。

ビットコインを使い、自分自身のノードを運用し、他の人々にお金の未来について学ぶ手助けをすることで、あなたは新たな世界に「投票」をしているのです。

アクティビティ：クラスディスカッションーあなたの視点はどう変わった？

以下の5つの質問に答えてください：



第10章

なぜお金が必要なのでしょうか？

お金とは何でしょうか？

なぜビットコインなのか？

お金をコントロールしているのは誰でしょうか？

お金に「価値」を与えてているのは何でしょうか？

第10章

第1章で選ばれた生徒たちの質問を書き出し、それに答えてみましょう。

- 1** 第1章の最初のアクティビティに戻り、今の自分の答えと以前の答えを比べてみましょう。
- 2** 元の回答と質問を比較し、話し合ってみましょう。何か変化はありましたか？
- 3** 最後にこの問い合わせ自分に投げかけてみてください。
「次のステップは何か？」
「この新しい知識を、どう活かして自分自身の力にできるか？」



次のステップに進みたくなったら、以下のセクションを見てみてね！さらなる学びと成功のために、選りすぐりのリソースを紹介しているよ。

追加資料

1.なぜビットコインを使うのか？

a “The Bullish Case for Bitcoin” – Vijay Boyapati

この論考では、ビットコインがなぜ価値ある資産であり、なぜ世界的な基軸通貨となる可能性を秘めているのかを論じています。著者はビットコインの技術的・経済的側面を解説し、それが強力な投資機会となる理由を明らかにしています。

b “Why Bitcoin Matters” – Aleks Svetski (動画・約1時間)

この動画では、分散型デジタル資産としてのビットコインの重要性と、それが現在の金融システムにどのように影響を与えるかについて語られています。講演者はビットコインが世界中の人々に経済的自由をもたらす可能性についても掘り下げています。

c “Why Bitcoin” – Wiz

この論文では、ビットコインを通貨や価値の保存手段として使う利点について概説されています。特に、ビットコインの分散型の性質がもたらす、より大きな経済的自由と安全性について強調されています。

2.ビットコインとは何か？

a “How Bitcoin Works under the Hood” – CuriousInventor (動画)

<https://www.youtube.com/watch?v=Lx9zgZCMqXE>

この動画では、ビットコインの技術的な構造や動作の仕組みについて詳しく解説しています。

b “What Is Bitcoin” – Greg Walker

この論文は、ビットコインの定義・歴史・技術的背景、そして従来の通貨との違いについて包括的に解説しています。

c “Bitcoin - The Genesis” – RT (動画・30分)

この動画では、ビットコインの誕生と初期の歴史を取り上げています。サトシ・ナカモトという謎の創設者の動機や、ビットコインという概念がどのように進化していったのかを探ります。

3.さらなる学習

a “The Bitcoin Standard”

(オーディオブック・約1時間40分)

このオーディオブックでは、ビットコインが誕生した経済的・歴史的背景を探り、分散型通貨の利点や、ビットコインがグローバルスタンダードになる可能性について論じています。

c “Bitcoin Babies” – Naomi Wambui

<https://bitcoinbabies.com/>

Twitter: @btcbabies / @ngachanaomi1

栄養・ビットコイン・メンタルヘルスなどの重要な知識を母親に提供することを目的とした、無料のPDFリソースです。

b “Intro to Bitcoin Austrian Thought”

(音声講義・約1時間)

この音声講義では、オーストリア学派経済学とビットコインの関係性を深掘りしています。ビットコインの背後にある経済原則や思想を学べます。

BTC Sessions

ビットコイン専用の教育系YouTubeチャンネルで、チュートリアルやガイドが豊富に揃っています。

<https://www.youtube.com/@BTCSessions>

4.コース：

a Summer of Bitcoin

大学生にビットコインのオープンソース開発とデザインを紹介することに焦点を当てた、グローバルなオンライン夏季インターンシッププログラムです。

b Chaincode Labs

<https://learning.chaincode.com/#FOSS>

オンラインコースとレジデンシー（研修）プログラムを通じて、ビットコインのプロトコル開発に必要なスキルを学べます。

c Saylor Academy

さまざまな分野にわたる無料の教育コンテンツを提供しています。

5. 重要な著者たち

- a Alex Gladstein: Check Your Financial Privilege
- Alex Swan: Grounded-Encounter Therapy:
- b Perspectives, Characteristics, and Applications
- c Amanda Cavalieri: Bitcoin and the American Dream: The New Monetary Technology Transcending Our Political Divide
- Anita Posch: Learn Bitcoin: Become Financially Sovereign
- Eric Yakes: The 7th Property: Bitcoin and the Monetary Revolution

- d Jeff Booth: The Price of Tomorrow: Why Deflation is the Key to an Abundant Future
- g Jimmy Song: The Little Bitcoin Book: Why Bitcoin Matters for Your Freedom, Finances, and Future
- i Nik Bhatia: Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies
- j Robert Breedlove: Thank God for Bitcoin: The Creation, Corruption, and Redemption of Money
- k Lyn Alden: Broken Money

6. 本文中で引用された著者

a Curious Inventor:

<https://www.youtube.com/@CuriousInventor>

b Anil Patel:

Twitter: @anilsaidso

7. その他の参考資料

- 1 Bitcoin.org
ビットコイン・プロトコルのウェブサイト。
- 2 Bitcointalk.org
ビットコイン関連の話題を議論したり、質問や情報共有を行ったりできるフォーラム。ビットコイン愛好家や専門家から学ぶのに最適です。
- 3 Bitcoincore.org
オリジナルのビットコインソフトウェア。現在多くのユーザーと開発者に使われています。ビットコインネットワークとのやり取りやアプリ構築に使える強力なツールセットを提供しています。
- 4 Bitcoinwiki.org
コミュニティ主導で運営されているビットコイン情報の総合ガイド。技術的な内容から歴史・活用事例まで幅広くカバーしています。
- 5 Bitcoinmagazine.com
ビットコインやその他の暗号資産に関するニュースや解説を提供するオンラインメディア。最新の動向を知るのに役立ちます。
- 6 Bitcoin.Design
ビットコイン関連のイラスト・ウェブ素材・テンプレート・アイコンなどを収録した、デザインファイルのオープンソースリポジトリ。
- 7 Yzer: <https://yzer.io/>
シンプルでモバイル対応のビットコイン教育プラットフォーム。ビットコイン・経済・金融について学びながらsatsを獲得できます。
- 8 NOSTR: <https://nostr.com/>
自分のデータを自分で所有できる分散型ソーシャルメディア。
- 9 Simple X: <https://simplex.chat/>
プライベートで分散型のアプリケーションプロトコル。
- 10 Set up a Bitcoin Node (Raspberry Pi DIY by Keith Mukai)
https://github.com/kdmukai/raspbpi4_bitcoin_node_tutorial?tab=readme-ov-file
- 11 How to select a Bitcoin wallet:
<https://bitcoin.org/en/choose-your-wallet>
新しく得た知識を使って、自分に合ったウォレットを選びましょう。
- 12 BitcoinIcons.com : <https://bitcoinicons.com/>
無料で使えるビットコインアイコン集。
- 13 Bitcoin For Local Business: <https://bitcoinforlocalbusiness.com/>
お気に入りの地元企業とビットコインの価値を共有するのに役立つチラシのセット。
- 14 Mempool.Space : <https://mempool.space/>
オープンソースのmempoolプロジェクト。ライトニングネットワークのデータやグラフも確認できます。

各章のコンセプト

第1章：

- コース紹介：**
 - ビットコイン・ディプロマの目標と期待される内容を学ぶ。
- 振り返り活動—お金の定義：**
 - お金に関する重要な質問に対して、5つの答えを自分なりに考えるワークに取り組む。
- クラスディスカッション—なぜお金が必要なのか：**
 - お金の基本的な必要性についてクラス全体で討論する。
 - お金の重要性について自分の意見を共有し、他の人の考えと比較する。
 - 経済システムにおけるお金の役割を理解するための基礎を築く。

第2章：

- お金の理解：**
 - お金の基本的な定義と概念を学ぶ。
 - クラス内で多様な視点を話し合い、お金の多面的な性質を理解する。
- お金の機能・性質・種類：**
 - お金の持つ機能・特性・種類を掘り下げて学ぶ。
 - これらの側面が、お金の定義と利用において重要であることを理解する。
- お金の心理学：**
 - お金に関する心理的な側面（希少性、時間選好、トレードオフ）を学ぶ。
 - 「時間選好」のアクティビティに取り組み、心理的要素と現実の生活との関係を理解する。

第3章：

- お金の歴史と進化の紹介：**
 - お金の歴史とその進化を学ぶ。
 - 古代の物々交換が、現在使っている通貨の発展にどのようにつながったのかを理解する。
- 通貨の進化：**
 - 貝殻やビーズなどの古代通貨から硬貨・紙幣への移行をたどる。
 - さらに、紙からプラスチックへの変遷を通じて、通貨の歴史的進化をたどる。
- デジタル通貨革命：**
 - お金の進化の最先端であるデジタル通貨について学ぶ。
 - 電子的な形でのみ存在し、即時かつ低成本な世界規模の取引を可能にする仕組みを理解する。
 - ビットコインがデジタル通貨の初期課題を解決する上で果たした役割を学ぶ。
- 物々交換ゲーム活動：**
 - 直接交換の難しさを体験する実践的なゲームに参加し、より効率的な仕組みの必要性を実感する。

第4章：

法定通貨の起源：

簡単な歴史的概要を通じて法定通貨の起源を学び、どのようにして主流の通貨形態となったかを理解する。

部分準備銀行制度アクティビティ：

部分準備銀行制度の仕組みを体験するアクティビティに参加し、このシステムが負債に依存していることや、経済全体への影響について理解を深める。

法定通貨（フィアット）システム：

法令によって成り立つ通貨システムとしての本質、部分準備銀行制度の役割、このシステムを管理する主要なプレイヤーについて理解を深める。

第5章：

購買力の低下：

通貨インフレという概念と、それが購買力に与える影響を学ぶ。「インフレの影響：オークション活動」に参加し、その影響を直接体験する。

法定通貨システムの影響アクティビティ：

「法定通貨システムの影響」アクティビティに参加し、現在の通貨システムがもたらす広範な影響について理解を深める。

中央銀行デジタル通貨（CBDC）：

中央銀行デジタル通貨（CBDC）の進化と、未来のお金に対する潜在的な影響を探る。

世界の負債と社会的不平等：

世界の負債と社会的不平等という二重の課題について探る。個人と社会の両方に及ぶ影響を理解し、購買力の低下や富の格差拡大を認識する。

サイファーパンクと分散化：

サイファーパンクの物語と、彼らが分散型通貨を求める動機を学ぶ。中央集権型システムと分散型システムの違いを理解し、デジタル通貨の簡単な歴史から洞察を得る。

第6章：

サトシ・ナカモトとビットコインの誕生：

サトシ・ナカモトという謎の人物とビットコインの誕生ストーリーを探り、その開発の背後にある初期の動機を理解する。

ビットコインの仕組み：

ナカモト・コンセンサス・メカニズムなど、ビットコインの仕組みを学ぶ。マイナー・ノード・ユーザー・開発者・プロジェクトなど、ネットワーク内で主要なプレイヤーがどのように協調して機能しているかを理解する。

クラスアクティビティ－コンセンサス構築：

「法定通貨システムの影響」アクティビティに参加し、現在の通貨システムがもたらす広範な影響について理解を深める。

健全なデジタルマネーとしてのビットコイン：

健全なデジタルマネーとしてのビットコインの役割を考察し、その進化・機能・特性について議論する。また、「ビットコインは健全なマネーかどうか」をテーマにクラスディスカッションを行う。

自己責任を受け入れる：

ビットコインの文脈における「自己責任」という概念の重要性をとらえ、分散型エコシステムにおける個人の役割と責任について理解を深める。

各章のコンセプト

第7章：

ピア・ツー・ピア取引：

分散型の取引に参加し、ビットコイン取引の基本原則を体験する。

ビットコインウォレットのセットアップ：

ビットコインウォレットを安全に利用するために、ダウンロード・鍵の作成・バックアップの基本手順を学ぶ。

貯蓄とDYOR：

価値の保存手段としてのビットコインでの貯蓄と、意思決定のために自分で調べること（DYOR／Do Your Own Research）の重要性を理解する。

第8章：

ライトニングネットワークの紹介：

ライトニングネットワークのような技術によってビットコインが進化し、機能が拡張してきたことを理解する。

ライトニングウォレットのセットアップ：

高速かつスケーラブルな取引を可能にするビットコイン・ライトニングウォレットの設定手順を学ぶ。

体験型アクティビティ：

ライトニングウォレットのリレーレースに参加し、ライトニングネットワークの取引について体感的に理解する。

第9章：

ビットコイン台帳：

ノードとマイナーによって維持される分散型台帳の概念を理解し、透明性とセキュリティの仕組みを学ぶ。

UTXOモデル：

ビットコインの取引プロセスの基礎である「未使用トランザクション出力（UTXO）モデル」を理解する。

公開鍵と秘密鍵：

公開鍵と秘密鍵による暗号学的セキュリティの重要性を学び、SHA-256ハッシュを使ったアクティビティを通じて理解を深める。

ビットコインウォレットの種類：

オープンソース・クローズドソース、カストディ型・非カストディ型ウォレットの違いと、鍵の管理がセキュリティにおいて果たす役割を学ぶ。

ビットコインの取得方法：

ピア・ツー・ピア取引や取引所などの方法を学び、KYC（本人確認）プロセスに関連するプライバシーの懸念について考える。

ライトニングウォレットの種類：

オープンソース・クローズドソース、カストディ型・非カストディ型ライトニングウォレットの違いを学び、ユーザーのニーズに応じたウォレットの選択肢を理解する。

ライトニング取引：

ライトニングネットワークを使った送金・受け取りのプロセスを学び、そのスピードと効率性を理解する。

ビットコインのノードとマイナー：

ノードとマイナーの役割を掘り下げ、発行・希少性・半減期・難易度調整といった側面を含めてネットワークの維持について学ぶ。

ビットコイン取引の仕組み：

ビットコインの取引ライフサイクルを、送信者・受信者・ノード・マイナー・mempoolといった要素の関係性を含めて理解する。mempoolの仕組みを体験するアクティビティにも取り組む。

第10章：

◆ ビットコインの哲学的基盤：

経済的課題への対応として、ビットコインがどのような思想のもとに生まれたかを探る。金融の自由に与える影響や、従来の通貨との違いにも注目しながら、その根本的な哲学を理解する。

◆ ビットコインの未来：

革新的なデジタル通貨としてのビットコインが、今後どのような方向に進む可能性があるのか、その将来性と発展の可能性を深掘りする。

◆ ディプロマの振り返り：

- ◆ ビットコイン・ディプロマ全体を通して得られた重要な学びをまとめ、自らの学習の道のりと得られた洞察について振り返る。
- ◆ アクティビティには、「なぜビットコインなのか？」というテーマの動画視聴や、第1章で出された問い合わせを再確認し、自身の理解がどれだけ深まったかを振り返る。

用語集

51%攻撃 (51% Attack):

ブロックチェーンネットワークに対する攻撃の一種で、1つの集団がネットワークの計算力の過半数を支配することで、取引の改ざんやネットワークの妨害を行うことが可能になる。

アルトコインシーズン (Altcoin Season):

ビットコイン以外の暗号資産の価格が大幅に上昇する期間。多くの場合、投資家の関心や採用の増加によって引き起こされる。

アルトコイン (Altcoins):

ビットコインを除くその他のデジタル通貨。

アトミックスワップ (Atomic Swap):

中央集権的な取引所や仲介者を介さずに、異なる暗号資産同士をユーザー同士で直接交換する仕組み。

オークション (Auction):

財や資産を最も高い価格を提示した者に売却する仕組み。

物々交換 (Bartering):

貨幣を用いずにモノやサービスを直接交換する行為。

バスケット・オブ・グッズ (Basket of Goods):

生活費の変動を測定するために使われる、複数の財やサービスの集合。

ビットコイン (Bitcoin):

銀行を介さずに入と人が直接お金を送れるようにするデジタル通貨・システム。

ブロックエクスプローラー (Block Explorer):

ブロックチェーン上のブロック、取引、ウォレットアドレスなどを閲覧できるツール。

ブロック報酬 (Block Reward):

新しいブロックをブロックチェーンに追加した際に、マイナーに与えられる新規発行されたビットコインの報酬。

ブロックチェーン (Blockchain):

これまでに行われたすべてのビットコイン取引の公開記録。

BTC (BTC):

ビットコインを表す単位記号（ティッカー）。購入や取引に利用できるデジタル通貨。

資本規制 (Capital Controls):

資金の国境を越えた移動に対して課される制限。

中央銀行 (Central Bank (Fed)):

国家の金融政策を担う政府所有の機関。

中央集権化 (Centralization):

権限や支配が一つの組織に集中すること。

中央集権型システム (Centralized System):

権限や制御が单一の主体に集中しているシステム。

コールドストレージ (Cold Storage):

ビットコインをハッカーやオンラインの脅威から隔離するために、オフラインで保管する方法。

商品貨幣 (Commodity Money):

金や銀のように、それ自体が価値を持ちつつ交換手段としても使われるモノ。

承認（Confirmation）：

取引がネットワークによって処理され、取り消される可能性が極めて低くなるまでのプロセス。マイナーやノードがコンピューターのハードウェアとソフトウェアを使って取引の正当性を検証する手段もある。二重支払いを防ぐためには、少なくとも6回の承認を待つことが推奨されている。

コンセンサスメカニズム（Consensus Mechanism）：

ブロックチェーン上の取引を検証・承認し、データの整合性を保つための仕組み。

暗号資産取引所（Cryptocurrency Exchange）：

ユーザーが暗号資産を法定通貨や他の暗号資産と売買・交換できるプラットフォーム。

暗号資産ウォレット（Cryptocurrency Wallet）：

秘密鍵を保管し、暗号資産の送受信や管理を行うためのソフトウェアや専用デバイス。

暗号技術（Cryptography）：

安全なシステムを構築するための数学分野。

通貨の希釈化（Debasement）：

硬貨に含まれる貴金属の量を減らすなどして、通貨の実質的な価値を下げるここと。

負債（Debt）：

他者に対して返済すべき金銭。

分散化（Decentralization）：

権限や管理を中央の組織に集中させず、ネットワーク全体に分散させること。

分散型自律組織（Decentralized Autonomous Organization (DAO)）：

スマートコントラクトによって運営され、中央管理者なしでブロックチェーン上で動作する組織やネットワーク。

分散型金融（Decentralized Finance (DeFi)）：

暗号資産業界において、中央機関を介さずにブロックチェーン上で動作する金融商品やサービスを構築しようとする取り組み。

分散型システム（Decentralized System）：

権限や制御が複数の主体に分散されているシステム。

デジタル資産（Digital Asset）：

価値の保存や交換手段として使える、価値をデジタルで表現したもの（例：ビットコイン）。

分散型台帳（Distributed Ledger）：

中央のサーバーに依存せず、ネットワーク上の複数のコンピューターに分散して保持されるデータベース。

欲求の二重の一一致（Double Coincidence of Wants）：

物々交換経済において、双方が互いに欲しいものを持っている状態。

二重支払い（Double Spend）：

同じビットコインを同時に別の相手に送ろうとする行為。

ダストトランザクション（Dust Transaction）：

送金額があまりにも小さく、手数料などを考慮すると経済的に成立しない取引。

為替レート（Exchange Rate）：

ある通貨の価値を、別の通貨に対して表したもの。

用語集

FOMO (FOMO) :

Fear of missing out (取り残されることへの恐怖) の略。暗号資産市場において、利益を得る機会を逃してしまうことへの不安や後悔の感情を指す言葉。

FUD (FUD) :

Fear, uncertainty, and doubt (恐怖・不確実性・疑念) の略。市場にパニックや価格下落を引き起こす否定的な噂や情報を指す。

国内総生産 (GDP) :

一定期間内に国内で生産された財やサービスの総価値。

ハードフォーク (Hard Fork) :

ビットコインのプロトコルを変更し、以前のバージョンと互換性のない新しいブロックチェーンを作成すること
(例: ビットコインキャッシュ)。

ハードウェアウォレット (Hardware Wallet) :

秘密鍵を保管し暗号資産を管理するための物理デバイス。ソフトウェアウォレットよりも高いセキュリティを提供する。

ハッシュ関数 (Hash Function) :

任意の長さの入力データから固定長の文字列を出力する数学的関数。暗号技術やブロックチェーン技術で広く使われている。

ハッシュレート (Hash Rate) :

ビットコインネットワークの処理能力を測定する指標。

HODL (ホドル) :

暗号資産を長期保有し、売買せずに持ち続けることを表すコミュニティ用語。「Hold」の綴り間違いから生まれた。

ホットウォレット (Hot Wallet) :

インターネットに接続されたビットコインウォレット。即時アクセスが可能だが、セキュリティリスクもある。

輸入 (Imports) :

他国で生産された財やサービスを自国市場で販売すること。

インフレーション (Inflation) :

経済全体における財やサービスの一般的な物価水準の上昇。

ICO (新規コイン公開／イニシャル・コイン・オファリング) :

新たに発行される暗号資産を、既存の暗号資産(例:ビットコイン)と引き換えに投資家に販売する資金調達手法。

レイヤー1プロトコル (Layer-1 Protocol) :

ブロックチェーンネットワークの基盤となる層で、合意形成・取引の検証・データの保存といった基本機能を担う。

レイヤー2プロトコル (Layer-2 Protocol) :

レイヤー1のブロックチェーン上に構築された第二層の仕組みで、スケーラビリティや速度、機能性を高める目的で使われる。

台帳 (Ledger) :

金融取引の記録。

ライトニングネットワーク (Lightning Network) :

ビットコインの小額取引をオフチェーンで処理することで、より高速かつ低コストの送金を可能にするレイヤー2の決済プロトコル。

MoE (交換手段／Mediums of Exchange) :

財やサービスと引き換えに広く受け入れられるモノや仕組み。

マークルツリー (Merkle Tree) :

ビットコインのブロックチェーンで使用される、データの整合性を効率よく検証するためのツリー状のデータ構造。

マイニングプール (Mining Pool) :

マイナーが協力して新しいブロックを見つける確率を高め、報酬を分配するために形成するグループ。

マイニング (Mining) :

ビットコインネットワークのためにコンピューターで数学的計算を行い、取引を承認しネットワークのセキュリティを高めるプロセス。

金融政策と財政政策 (Monetary and Fiscal Policy) :

それぞれ中央銀行と政府が実施する、通貨供給量や金利に影響を与える経済政策。

マネーサプライ (Money Supply) :

経済全体に流通している通貨の総量。

マルチシグウォレット (Multi-Signature (Multisig) Wallet) :

1つのトランザクションを実行するために、複数の署名または承認が必要となるウォレット。セキュリティや管理の強化につながる。

マルチシグ (マルチシグネチャ／Multi-Signature) :

ビットコイントランザクションの承認に複数の秘密鍵を必要とするセキュリティ機能。

ネットワーク (Network) :

相互に接続された複数の主体の集合。

ノードネットワーク (Node Network) :

ビットコインネットワークを支え、維持するために相互接続されたコンピューターやデバイスのネットワーク。

ノード (Node) :

ビットコインネットワークに接続され、取引の検証や伝達に参加するコンピューターまたはデバイス。

非代替性トークン (Non-Fungible Token／NFT) :

デジタル資産の一種で、アートやコレクションなど唯一無二の価値を持つアイテムを表現するために使われる。

ナンス (Nonce) :

ブロックのハッシュ値が難易度ターゲットを満たすように調整される、ブロックヘッダーに追加されるランダムな数値。

孤立ブロック (オーファンブロック／Orphan Block) :

他のより長いチェーンに無効化されたため、ブロックチェーンの主チェーンに含まれなかったブロック。

ペーパーウォレット (Paper Wallet) :

暗号資産をオフラインで保管・管理するために、秘密鍵と公開鍵を紙に印刷したもの。

ピア・ツー・ピア (Peer-to-Peer／P2P) :

中央の管理者を介さず、参加者同士が直接やり取りする分散型ネットワーク。

用語集

ペッグ（Peg）：

ある通貨の価値を他の通貨に固定する為替制度。1つの通貨が別の通貨の価値に連動するよう設定される。

プライベートブロックチェーン（Private Blockchain）：

分散化されておらず、単一の組織によって管理されているブロックチェーン。

秘密鍵（Private Key）：

特定のウォレットからビットコインを送金する権利を証明する秘密のデータ。暗号署名によってその所有権を証明する。

プルーフ・オブ・ステーク（Proof-of-Stake／PoS）：

一部のブロックチェーンネットワークで採用されているコンセンサスメカニズムで、取引の検証に参加するには一定量の暗号資産を保有する必要がある。

プルーフ・オブ・ワーク（Proof-of-Work）：

ネットワークに参加するために、一定量の計算作業を行うことを求めるコンセンサスメカニズム。

パブリックブロックチェーン（Public Blockchain）：

誰でも参加して取引を検証できる、分散型のブロックチェーン。

公開鍵（Public Key）：

秘密鍵から数学的に導出され、ビットコインの受け取りに使われる一意の識別子。

公開鍵／ビットコインアドレス（Public Key／Bitcoin Address）：

ビットコインの受け取りに使う公開の文字列や識別番号。

公開台帳（Public Ledger）：

すべての取引記録を公開・分散型で管理するビットコインネットワーク上のデータベース。

購買力（Purchasing Power）：

お金で財やサービスを購入できる力。

リカバリーフレーズ／シードフレーズ（Recovery Phrase／Seed Phrase）：

複数の秘密鍵と公開鍵のペアを生成できる、12語・18語・24語の単語列。ビットコインウォレットの復元に使用される。

預金準備率（Reserve Ratio）：

銀行が預金のうち、現金や準備金として保有しなければならない割合。

銀行制度へのアクセス制限（Restrictive Banking）：

銀行サービスや口座アクセスに対して課される制限や制約。

サトシ・ナカモト（Satoshi Nakamoto）：

ビットコインを生み出した匿名の創設者が使用していた仮名。

Satoshi（サトシ／sats）：

ビットコインの最小単位で、1ビットコインの1億分の1。ビットコインの創設者であるサトシ・ナカモトにちなんで名付けられている。

sat/vB（satoshi per virtual byte）：

ビットコイン取引手数料の単位で、1バーチャルバイトあたりに支払われるSatoshi数を表す。

SegWit (セグウィット／Segregated Witness) :

ブロックチェーン上のデータの保存方式を変更することで、容量の拡張とトランザクション手数料の削減を可能にしたビットコインのプロトコルアップグレード。

サイドチェーン (Sidechain) :

別のブロックチェーンと接続され、資産や情報を相互に移転できるブロックチェーン。

署名 (Signature) :

所有権を証明するための数学的な仕組み。

スマートコントラクト (Smart Contract) :

契約内容がコードとして記述され、自動的に実行されるプログラム。

ソフトフォーク (Soft Fork) :

古いバージョンのソフトウェアとも互換性を保ったままプロトコルを変更する方法。

ステーブルコイン (Stablecoin) :

法定通貨やその他の資産に価値を連動させることで、価格の安定を目指す暗号資産。

需要と供給 (Supply and Demand) :

財やサービスの価格は、その供給量と需要量の相互作用によって決まるという経済原則。

貨幣の時間的価値 (Time Value of Money) :

同じ金額であっても、将来よりも現在の方が価値があるという考え方。

トークン (Token) :

特定のブロックチェーン上で作られた価値の単位で、特定の資産や機能を表すのに使われることが多い。

トークン化 (Tokenization) :

資産や資産クラスをブロックチェーン上にデジタルで表現するプロセス。分割所有や移転を可能にする。

取引ペア (Trading Pair) :

暗号資産取引所において、売買や交換が行われる2つの通貨または資産の組み合わせ。

トランザクション手数料 (Transaction Fee) :

送信者がマイナーへの報酬として支払う少額のビットコイン。トランザクションがブロックに取り込まれることを促す。取引手数料とも呼ばれる。

トランザクションID (Transaction ID) :

ビットコインの送金内容（送金額・送信先と送信元のアドレス・日時など）を特定する文字と数字の組み合わせ。

トランザクション (Transaction) :

ビットコインネットワーク上で、あるアドレスから別のアドレスへビットコインを送ること。

トラストレス (Trustless) :

第三者や仲介者への信頼を必要とせず、技術的な仕組みの透明性と安全性によって成り立つシステムや取引。

用語集

二要素認証（Two-Factor Authentication／2FA）：

パスワードに加え、別のコードやデバイスによる認証を必要とするセキュリティ対策。アカウントや取引へのアクセス時に使用される。

アンバンクト（Unbanked）：

従来型の銀行サービスを利用できない個人やコミュニティ。

価値の尺度（Unit of Account）：

財やサービスの価値を表すための共通の測定単位。

ボラティリティ（Volatility）：

資産価格の変動の度合い。時間とともに価格がどれだけ上下するかを示す。

ウォレットアドレス（Wallet Address）：

ビットコインの送受信に使われる一意の識別子。英数字の文字列で表される。

ウォレットバックアップ（Wallet Backup）：

ビットコインウォレットのリカバリーフレーズ（または秘密鍵）のコピー。紛失や盗難時の復元に使用される。

ウォレット（Wallet）：

ビットコインを保管・管理する仮想的な「財布」。ブロックチェーン上のビットコインを使用するための秘密鍵が含まれている。

クジラ（Whale）：

大量の暗号資産を保有し、大規模な売買によって市場価格に影響を与える可能性のある個人または組織。

ホワイトハッカー（White Hat Hacker）：

セキュリティ上の脆弱性を見つけて修正する、倫理的なハッカー。

ホワイトペーパー（Whitepaper）：

ブロックチェーンプロジェクトや暗号資産が解決しようとする課題とその解決策を説明した文書。

XBTとBTC（XBT and BTC）：

どちらもビットコインを表す略称。BTCが一般的に使用されるが、XBTは国際通貨コード規則に準じた表記。

Independent because of you!

あなたのおかげで、自立できた！

THANKS TO THE DONORS WHO CONTRIBUTED TO OUR GEYSER CAMPAIGN OR AT ADOPTING BITCOIN 2024



Thank you!



日本語版 | 2025年版